CA ARCserve® Central Virtual Standby

Guida per l'utente

r16.5

Riferimenti ai prodotti CA Technologies

Questo documento è valido per i seguenti prodotti di CA Technologies:

- CA ARCserve® Backup
- CA ARCserve® D2D
- CA ARCserve® Replication e High Availability
- CA ARCserve® Central Host-Based VM Backup
- CA ARCserve® Central Protection Manager
- CA ARCserve® Central Reporting
- CA ARCserve® Central Virtual Standby

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Collegamenti di supporto per CA ARCserve Central Applications:

CA Support Online offre un insieme di risorse per la risoluzione di problemi tecnici e fornisce l'accesso a informazioni di prodotto importanti. Il CA Support consente di accedere facilmente a fonti di supporto disponibili in qualunque momento. I seguenti collegamenti consentono l'accesso a vari siti di CA Support disponibili per l'utente:

- **Informazioni sul Supporto tecnico** - Questo collegamento fornisce informazioni sui programmi di manutenzione e le offerte di supporto, inclusi termini e condizioni, richieste, obiettivi del livello di servizio e ore di servizio.

  https://support.ca.com/prodinfo/centappssupportofferings

- **Registrazione al Supporto tecnico** - Questo collegamento consente di accedere al modulo di registrazione in linea di CA Support, utile per l'attivazione del supporto per il prodotto.

  https://support.ca.com/prodinfo/supportregistration

- **Accesso al Supporto tecnico** - Questo collegamento consente di accedere alla pagina del supporto One-Stop di CA ARCserve Central Applications.

  https://support.ca.com/prodinfo/arccentapps

Modifiche apportate alla documentazione

Di seguito sono riportati gli aggiornamenti apportati alla documentazione dall'ultima release di CA ARCserve Central Virtual Standby:

- Aggiornamento contenente commenti e suggerimenti degli utenti, correzioni e altre modifiche minori per migliorare le modalità di utilizzo e il funzionamento del prodotto o la documentazione stessa.
- Aggiunta della sezione Creazione di uno scenario di CA ARCserve Replication and High Availability per Virtual Standby remoto (a pagina 17). Questo argomento descrive la procedura per la creazione di scenari di CA ARCserve D2D e CA ARCserve Central Host-Based VM Backup da CA ARCserve Replication and High Availability durante la creazione del criterio remoto di Virtual Standby.
- Aggiunta della sezione Importazione dei nodi da CA ARCserve Replication (a pagina 39). Questa sezione descrive la procedura per l'importazione di più da CA ARCserve Replication.
- Aggiunta della sezione Configurazione di convertitori remoti (a pagina 39). Questa sezione descrive la procedura di conversione dei punti di ripristino di CA ARCserve D2D per registrarli automaticamente con Microsoft Hyper-V, VMware vCenter o ESXi.
- Aggiornamento della sezione Creazione di criteri in Creazione dei criteri CA ARCserve Central Virtual Standby (a pagina 40). Questa sezione è stata aggiornata per includere due tipi di criteri che possono essere creati dall'utente: criteri locali e remoti di Virtual Standby.
- Aggiornamento della sezione Attività di gestione dei nodi (a pagina 63). Questa sezione è stato aggiornato per includere l'opzione Importa nodi da CA ARCserve Replication.
- Aggiunta della sezione Impostazione delle password di backup per uno o più nodi di CA ARCserve D2D (a pagina 66). Questo argomento descrive la procedura per impostare una o più password di backup di CA ARCserve D2D e trasferirle al convertitore presente sul sito MSP.
- Aggiornamento della sezione Modifica o copia di criteri (a pagina 76). Questa sezione è stata aggiornata per includere i due tipi di criteri disponibili per la copia o la modifica.
- Aggiornamento della sezione Visualizzazione registri (a pagina 83). Questa sezione è stata aggiornata per includere le seguenti opzioni del modulo: Interrompi/Riprendi heartbeat, Interrompi/Riprendi Virtual Standby, Aggiorna nodi multipli, Computer virtuale di standby e Importa nodi da CA ARCserve Replication.
- Aggiunta della sezione Attivazione dei computer virtuali di Virtual Standby (a pagina 111). Questa sezione descrive la possibilità di avviare il computer virtuale Virtual Standby localmente (a pagina 111) e in remoto (a pagina 118).

- Aggiunta della sezione Gestione del menu delle operazioni di ripristino bare metal (a pagina 146). Questa sezione descrive i tre tipi di operazioni di ripristino bare metal.
- Aggiornamento della sezione Errore di accesso negato con l'aggiunta di un nodo per IP/Nome (a pagina 188). Questa sezione è stata aggiornata per includere due soluzioni per disabilitare il Controllo account utente (UAC).
- Aggiunta della sezione Esclusione di file dalla scansione antivirus (a pagina 210). Questo argomento descrive i file, le cartelle e i processi da escludere prima della scansione antivirus.

Sommario

Capitolo 7: Ripristino dei dati 129

Capitolo 8: Risoluzione dei problemi di CA ARCserve Central Virtual Standby 171

Capitolo 1: Introduzione a CA ARCserve Central Virtual Standby

Questa sezione contiene i seguenti argomenti:

Introduzione

CA ARCserve Central Applications combina la protezione dei dati principali e le tecnologie di gestione con un ecosistema mirato di applicazioni che funzionano all'unisono al fine di facilitare la protezione, la copia, lo spostamento e la trasformazione dei dati on-premise e off-premise all'interno di ambienti globali.

Le applicazioni CA ARCserve Central Applications possono essere utilizzate, gestite e installate facilmente. Questa soluzione consente alle organizzazioni un controllo automatizzato delle informazioni al fine di prendere decisioni consapevoli sull'accesso, sulla disponibilità e sulla protezione dei dati in base al valore di business complessivo.

CA ARCserve Central Virtual Standby è un'applicazione offerta da CA ARCserve Central Applications. CA ARCserve Central Virtual Standby è integrato con CA ARCserve D2D e consente di eseguire il provisioning di computer virtuali a partire dalle sessioni di backup di CA ARCserve D2D. L'applicazione consente di eseguire le seguenti operazioni:

- Conversione dei punti di ripristino di CA ARCserve D2D archiviati nelle periferiche di destinazione di CA ARCserve D2D in formati VMware Virtual Disk (VMDK) o Microsoft Virtual Hard Disk (VHD) in base ad una pianificazione. Dalle snapshot dei punti di ripristino sarà possibile utilizzare i computer virtuali come server di origine di CA ARCserve D2D in caso di errore dei server di origine.
- Distribuire i criteri di conversione ai server di origine di CA ARCserve D2D.
- Archiviare snapshot dei punti di ripristino su computer virtuali basati sul server VMware ESX o Windows Hyper-V.
- Attivare i computer virtuali manualmente o automaticamente in caso di emergenza.
- Eseguire recuperi dei dati da snapshot del punto di ripristino sui server di origine originali o alternativi (ripristini V2P).

Modalità di funzionamento di CA ARCserve Central Virtual Standby

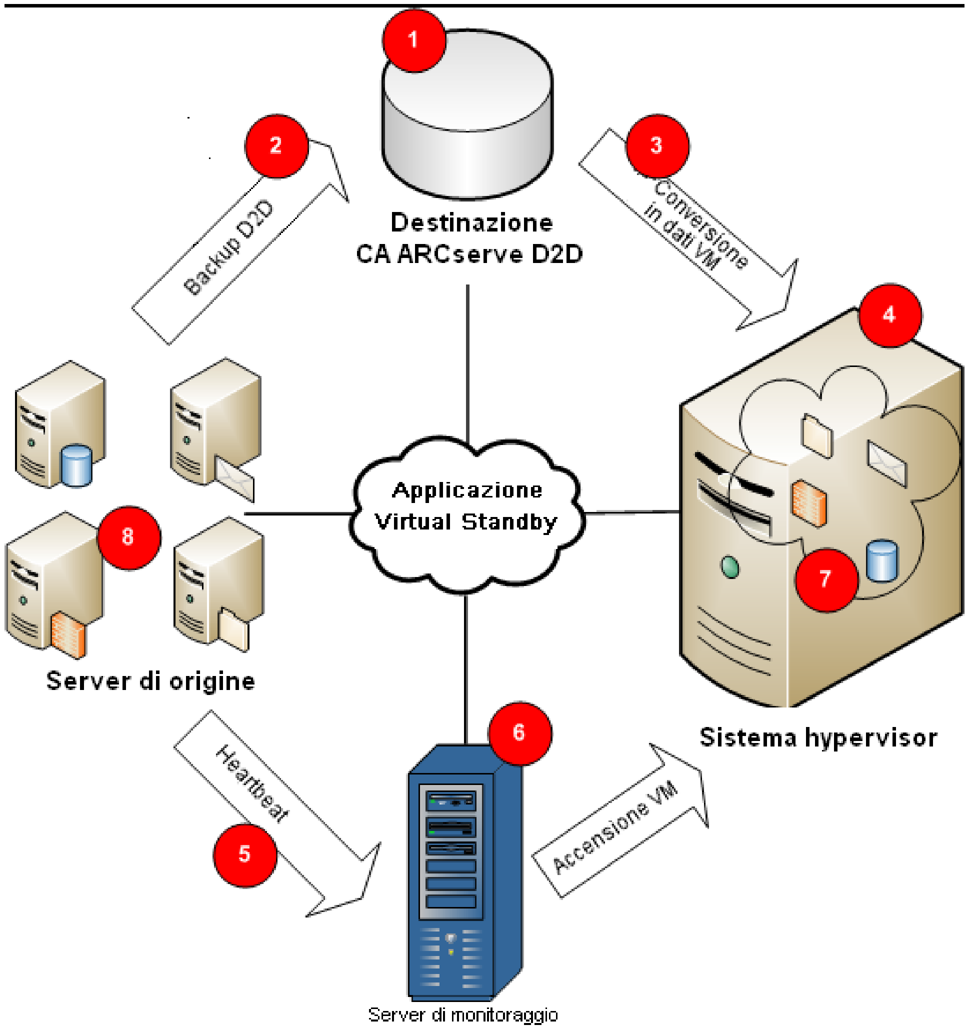
Virtual Standby consente di proteggere i server di origine di CA ARCserve D2D eseguendo le operazioni riportate a continuazione:

- Conversione dei punti di ripristino di CA ARCserve D2D archiviati nelle periferiche di destinazione di CA ARCserve D2D in formati VMware Virtual Disk (VMDK) o Microsoft Virtual Hard Disk (VHD) in base ad una pianificazione.
- Copia dei dati convertiti su un sistema hypervisor.
- Creazione di snapshot del punto di ripristino dai dati VMDK o VHD del computer virtuale.
- Controllo dello stato del server di origine.
- Attivazione automatica dei computer virtuali da snapshot del punto di ripristino in caso di emergenza.

  Nota: in Virtual Standby è possibile configurare l'attivazione automatica o manuale delle snapshot del punto di ripristino in caso di errore.

- Recupero dei dati dal computer virtuale al server di origine, dopo la correzione dei problemi sul server di origine.

Il diagramma seguente illustra questo processo:



CA ARCserve D2D (1) crea i punti di ripristino sulla periferica di destinazione di CA ARCserve D2D (2) per i server di origine. Virtual Standby converte i punti di ripristino al formato del computer virtuale (3) e archivia i dati come snapshot del punto di ripristino sul sistema hypervisor (4).

Il server di monitoraggio (6) controlla lo stato dei server di origine. Se il server di monitoraggio non riesce ad individuare un heartbeat (5) da un server di origine (8), il server di monitoraggio attiverà un computer virtuale con thin provisioning (7) sul sistema hypervisor (4). Tale computer virtuale fungerà da server di origine utilizzando i dati contenuti nella snapshot del punto di ripristino più recente. CA ARCserve Central Virtual Standby crea una partizione del computer virtuale della stessa dimensione del server di origine.

Dopo aver risolto i problemi sul server di origine, è possibile recuperare il server di origine (8) allo stato corrente utilizzando i dati (7) archiviati nel computer virtuale sul sistema hypervisor.

Nota: se si desidera eseguire il backup del computer virtuale dopo la sua attivazione, effettuare la distribuzione di un criterio di backup di CA ARCserve D2D sul computer virtuale utilizzando CA ARCserve Central Protection Manager.

Bookshelf di CA ARCserve Central Applications

Gli argomenti contenuti nella Guida in linea di CA ARCserve Central Applications sono disponibili anche nella Guida per l'utente in formato PDF. La versione PDF più recente di questa guida e la Guida in linea sono accessibili dal Bookshelf di CA ARCserve Central Applications.

Nei file Note di rilascio di CA ARCserve Central Applications sono contenute informazioni relative ai requisiti di sistema, al supporto di sistemi operativi, al supporto per il recupero delle applicazioni e altre informazioni che può essere necessario conoscere prima di installare il prodotto. I file di Note di rilascio contengono inoltre un elenco di problemi noti di cui l'utente deve essere a conoscenza prima di utilizzare CA ARCserve Central Applications. La versione più recente delle note di rilascio è disponibile nel Bookshelf di CA ARCserve Central Applications.

Capitolo 2: Installazione di CA ARCserve Central Virtual Standby

Questa sezione contiene i seguenti argomenti:

Attività preliminari all'installazione

Prima di installare CA ARCserve Central Virtual Standby, completare le seguenti operazioni preliminari:

- Verificare che la versione supportata più recente di CA ARCserve D2D sia installata su:
  - I server di origine da proteggere
  - Il server specificato per l'archiviazione delle snapshot dei punti di ripristino

    Nota: questo requisito è valido solamente per i server Hyper-V configurati per il monitoraggio dello stato dei nodi (computer fisici o virtuali), e per l'archiviazione delle snapshot del punto di ripristino per i nodi.
  - Il server specificato per il monitoraggio dei server di origine

  Nota: se CA ARCserve Central Protection Manager è stato installato nell'ambiente di produzione, è possibile installare CA ARCserve D2D sui nodi remoti tramite la Distribuzione D2D. Per ulteriori informazioni, consultare la Guida per l'utente di CA ARCserve Central Protection Manager.
- Per gli ambienti Hyper-V, verificare che CA ARCserve D2D sia installato nel sistema host Hyper-V. In ambienti Hyper-V, i sistemi host Hyper-V agiscono da percorso di archiviazione per le snapshot del punto di ripristino e da server di monitoraggio.
- Per ambienti VMware, verificare che CA ARCserve D2D sia installato nel sistema proxy.

  Nota: in ambienti VMware, l'archivio dati del server ESX di destinazione funge da posizione di archiviazione delle snapshot del punto di ripristino. In alternativa, il sistema proxy può fungere da server di monitoraggio.

- Consultare il file delle Note di rilascio. Le Note di rilascio descrivono i requisiti di sistema, i sistemi operativi supportati e un elenco di problemi noti per questa versione.
- Verificare che il sistema soddisfi i requisiti minimi hardware e software necessari per l'installazione di CA ARCserve Central Virtual Standby.
- Verificare che l'account Windows disponga dei privilegi di amministratore o equivalenti per l'installazione del software sui computer nei quali si desidera installare CA ARCserve Central Virtual Standby.
- Verificare che l'account disponga dei privilegi di amministratore per server VMware vCenter o ESX e dei privilegi di amministratore di Windows. Per consentire il corretto completamento delle operazioni di VDDK, è necessario assegnare l'account al ruolo di licenza globale sul sistema server vCenter o ESX.
- Verificare di disporre dei nomi utente e delle password dei computer su cui si sta procedendo all'installazione di CA ARCserve Central Virtual Standby di cui si è in possesso.
- Verificare di disporre dei nomi host o dell'indirizzo IP dei computer selezionati per il monitoraggio dei computer di origine.
- Verificare di disporre dei nomi host o dell'indirizzo IP dei computer selezionati per l'archiviazione delle snapshot del punto di ripristino.
- Verificare di disporre di tutte le licenze necessarie per l'installazione di CA ARCserve Central Virtual Standby di cui si è in possesso.
- Verificare che il numero di versione di CA ARCserve D2D corrisponda a quello di CA ARCserve Central Virtual Standby.
- CA ARCserve Central Applications consente di installare CA ARCserve D2D e di eseguire l'aggiornamento della versione precedente all'ultima versione su nodi remoti mediante l'utilità di distribuzione. Per eseguire il backup dei dati sui nodi remoti utilizzando l'ultima versione di CA ARCserve D2D, è necessario disporre della versione più recente delle licenze di CA ARCserve D2D e applicare tali licenze sui nodi. Se le licenze non vengono applicate entro 31 giorni dalla data di installazione o di aggiornamento di CA ARCserve D2D sui nodi, il funzionamento di CA ARCserve D2D verrà interrotto.

Attività preliminari all'installazione di Virtual Standby remoto

Virtual Standby remoto consente di creare computer virtuali di Virtual Standby da sessioni di CA ARCserve D2D e CA ARCserve Central Host-Based VM Backup replicate.

Prima di utilizzare Virtual Standby per creare computer virtuali di Virtual Standby di sessioni di CA ARCserve D2D replicate, completare le attività preliminari nell'ordine seguente:

1. Installare CA ARCserve Replication and High Availability. Per ulteriori informazioni, consultare la Guida per l'utente di CA ARCserve Replication and High Availability.

   Importante. L'esecuzione di CA ARCserve Replication and High Availability durante le operazioni di Virtual Standby remoto richiede la licenza.

2. Configurare CA ARCserve D2D, CA ARCserve Central Host-Based VM Backup o entrambi per creare punti di ripristino. Per ulteriori informazioni, consultare la Guida per l'utente di CA ARCserve D2D oppure la Guida per l'utente di CA ARCserve Central Host-Based VM Backup.

3. Creare uno scenario di replica per eseguire la copia dei punti di ripristino in una posizione remota. Per ulteriori informazioni, consultare la sezione Creazione di uno scenario di CA ARCserve Replication and High Availability per Virtual Standby remoto (a pagina 17).

Creazione di uno scenario di CA ARCserve Replication and High Availability per Virtual Standby remoto

Virtual Standby consente di creare scenari di CA ARCserve Replication and High Availability per eseguire le copia dei punti di ripristino in una posizione remota.

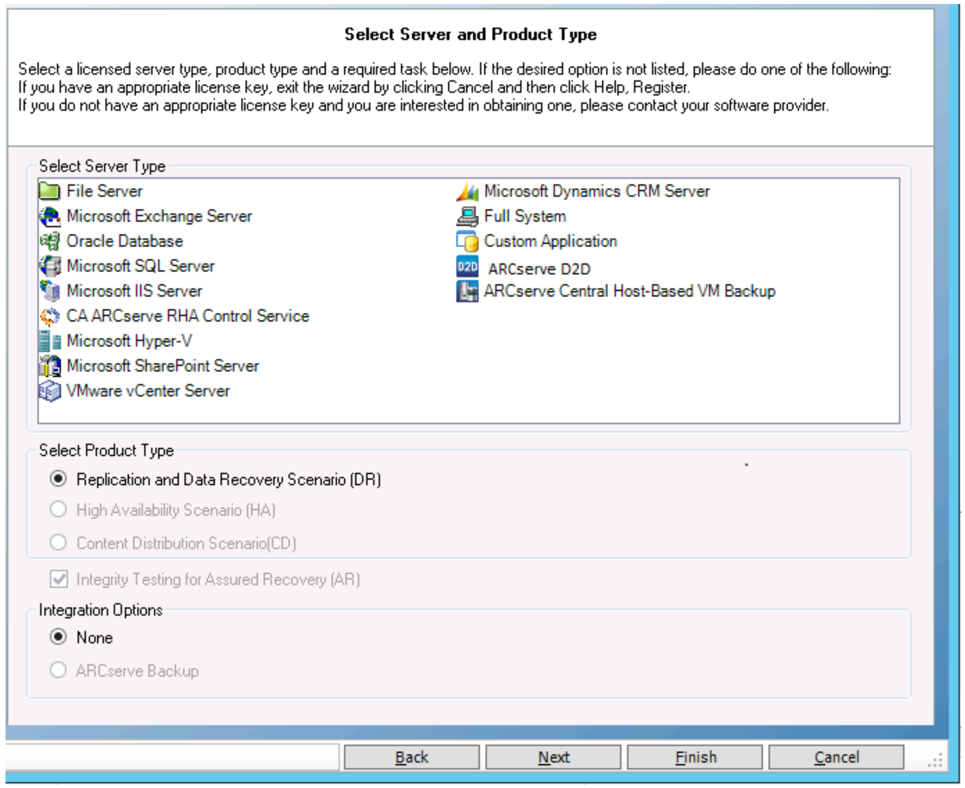
Procedere come descritto di seguito:

1. Aprire la Gestione di CA ARCserve Replication and High Availability. Dal menu Scenario, fare clic su Nuovo oppure fare clic sul pulsante Nuovo della barra degli strumenti standard.

   Viene visualizzata la schermata Introduzione della Creazione guidata dello scenario .

2. Selezionare Crea nuovo scenario

Viene visualizzata la schermata Selezione del server e del tipo di prodotto.



3. Selezionare le opzioni seguenti e fare clic su Avanti.

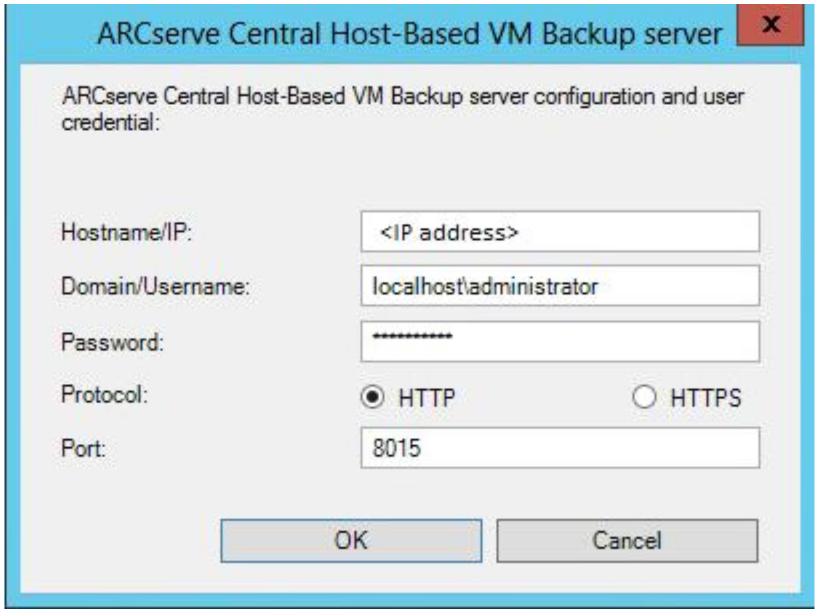
   a. Tipo di server: CA ARCserve Central Host-Based VM Backup

      Nota: i processi seguenti sono validi anche per CA ARCserve D2D.

   b. Tipo di prodotto: Scenario di replica e recupero dati (DR)

   c. Opzioni di integrazione: Nessuna

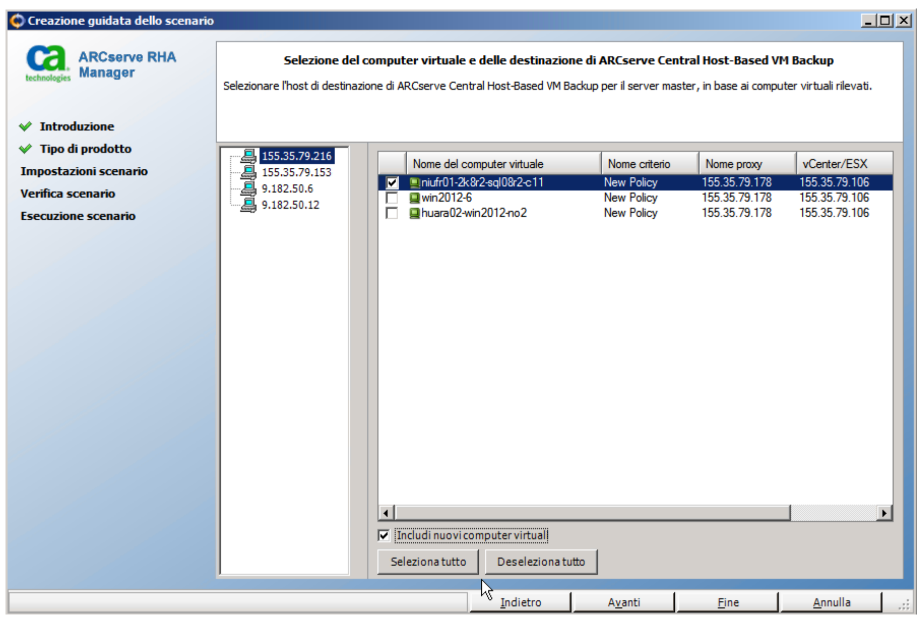
Viene visualizzata la finestra delle credenziali del server ARCserve Central Host-Based VM Backup.



4. Immettere le credenziali e fare clic su OK. Il nome del server viene compilato in base ai dati specificati nel passaggio 3.

   Viene visualizzata la schermata Selezione del computer virtuale e delle destinazione di ARCserve Central Host-Based VM Backup.

   Nota: questa schermata non è disponibile per gli scenari CA ARCserve D2D ed è visualizzata unicamente per gli scenari CA ARCserve Central Host-Based VM Backup.



CA ARCserve Replication and High Availability esegue la connessione al server CA ARCserve Central Host-Based VM Backup per acquisire il criterio e visualizzare gli host di destinazione di backup e i computer virtuali corrispondenti.

5. Selezionare il nome host e i computer virtuali che si desiderano proteggere.

   Includi nuovi computer virtuali : specifica che vengono replicate tutte le sottocartelle contenute nella cartella di backup dell'host principale quando si esegue questo scenario. Vengono inoltre replicate tutte le cartelle di backup dei computer virtuali appena create. Sono escluse solo le cartelle dei computer virtuali non selezionate. Tali cartelle vengono contrassegnate come da escludere. Se non si seleziona questa opzione, vengono replicate solo le cartelle di backup selezionate.

   I file di backup dei computer virtuali selezionati vengono replicati durante l'esecuzione dello scenario. Si tratta dei file di backup creati da CA ARCserve D2D.

6. Immettere i seguenti dati per il master e la replica:

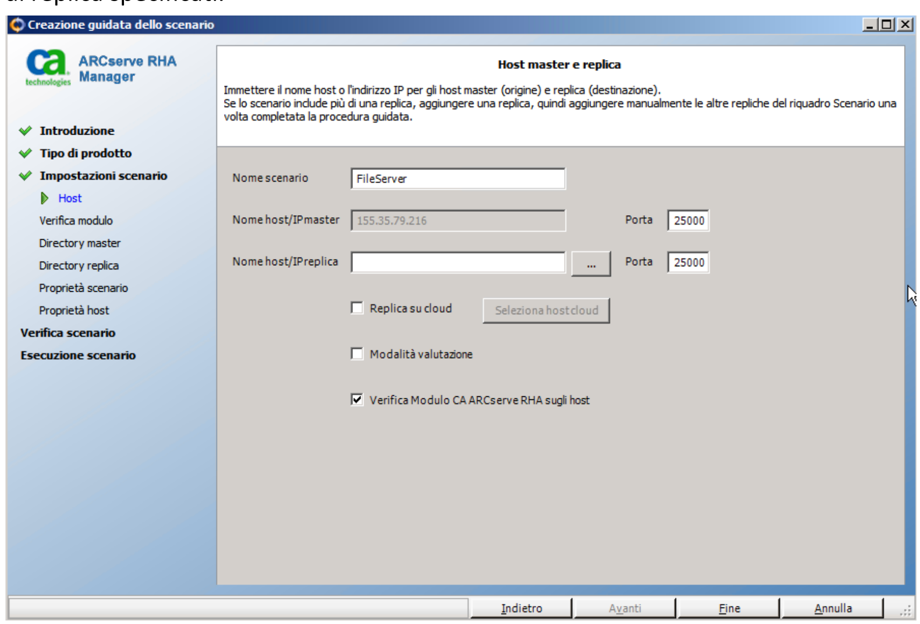
   Nome scenario: accettare il nome predefinito o immetterne un nome univoco.

   Nome host/IP master: questo campo viene compilato automaticamente in base al nome host selezionato.

   Nome host/IP replica: immettere il nome host o l'indirizzo IP del server di replica. Questo server corrisponde al server di destinazione. Utilizzare il pulsante Sfoglia per cercare un server di replica.

   Porta: accettare il numero di porta predefinito (25000) o immettere altri numeri di porta per il master e la replica.

   (Facoltativo) Verificare Modulo CA ARCserveRHA sugli host: selezionare questa opzione per verificare se i moduli sono installati e in esecuzione sugli host master e di replica specificati.



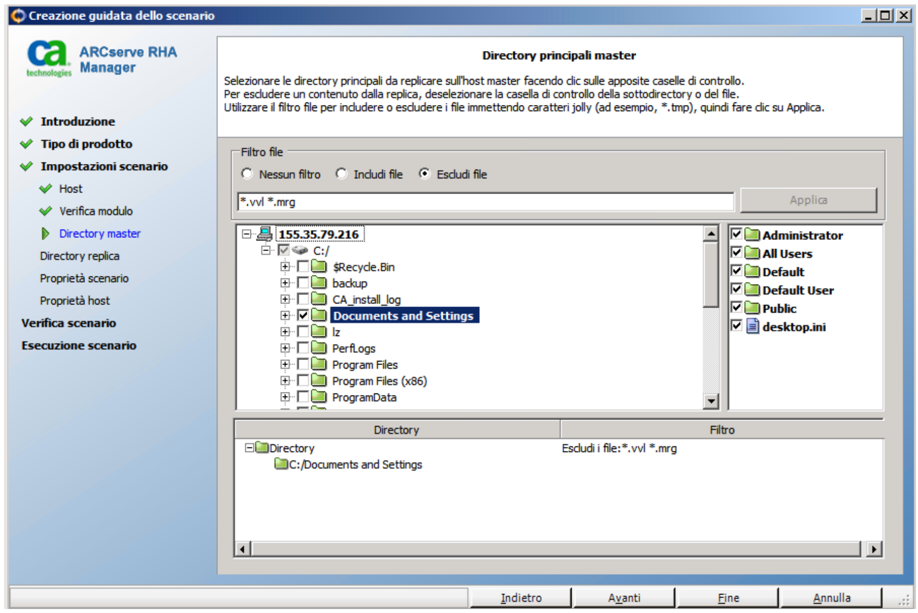
7. Fare clic su Avanti.

   Viene visualizzata la schermata Verifica modulo.

   Se l'opzione è stata abilitata, verrà visualizzata la schermata di verifica host. Il software verifica l'esistenza e la connettività degli host master e replica specificati nella schermata precedente.

8. Fare clic su Avanti.

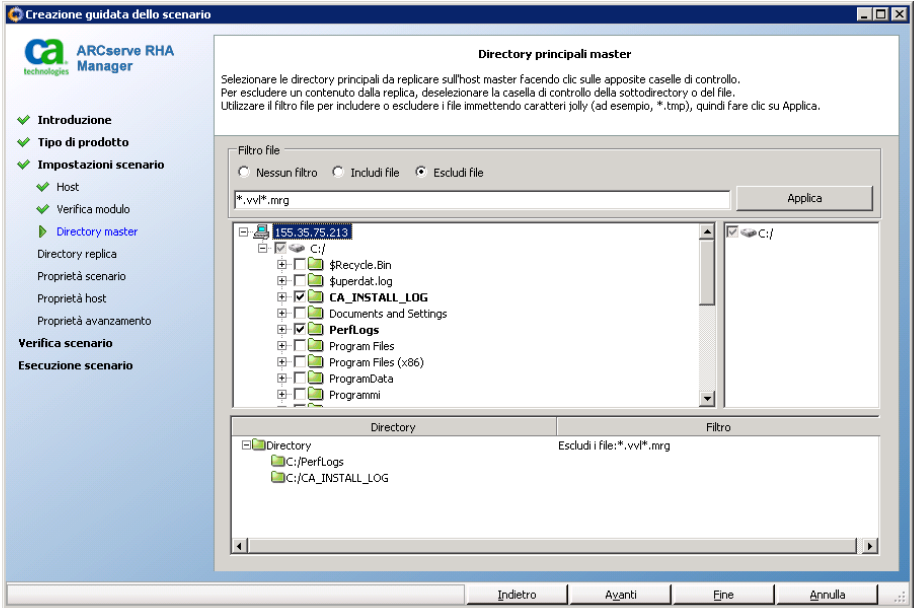
   Viene visualizzata la schermata Directory principali master.



Il modulo RHA rileva le cartelle di backup dei computer virtuali selezionati. Le cartelle di backup vengono selezionate automaticamente.

Nota: queste cartelle corrispondono alle cartelle di backup create da CA ARCserve D2D.

Quando si seleziona l'opzione Includi nuovi computer virtuali nella schermata Selezione del computer virtuale e della destinazione di CA ARCserve Central Host-Based VM Backup, la cartella di backup principale viene selezionata per la replica, mentre le cartelle escluse vengono elencate nel riquadro di filtro.



9. Fare clic su Avanti.

   Viene visualizzata la schermata Directory principali di replica.

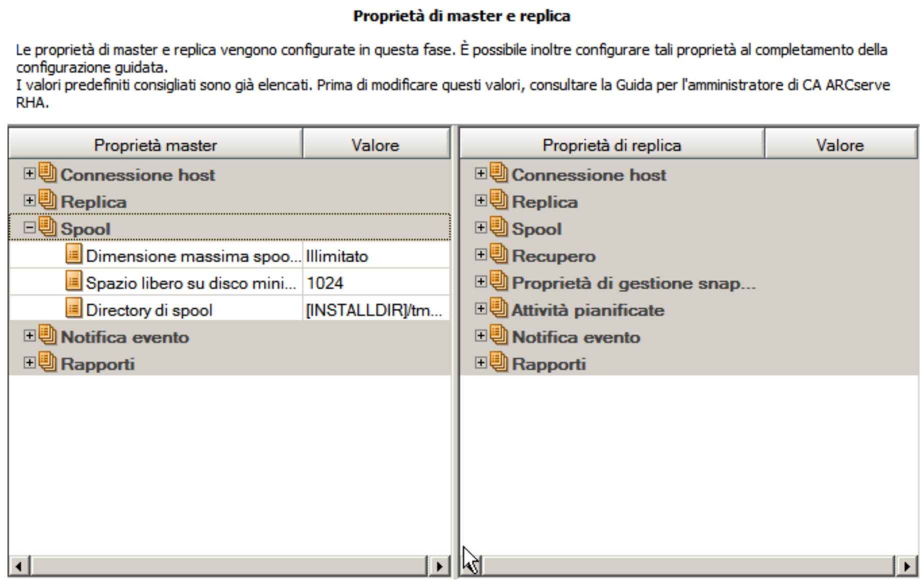
10. Accettare le impostazioni predefinite e fare clic su Avanti.

    Viene visualizzata la schermata Proprietà scenario.

11. Configurare le proprietà riguardanti l'intero scenario. Per questo esempio, accettare semplicemente le impostazioni predefinite. È possibile configurare queste proprietà senza utilizzare la procedura guidata. Per ulteriori informazioni sulla configurazione delle proprietà dello scenario, consultare la sezione Configurazione delle proprietà di uno scenario.

12. Fare clic su Avanti.

    Viene visualizzata la schermata Proprietà di master e replica.



13. Configurare le proprietà relative agli host master o di replica. Per questo esempio, accettare semplicemente le impostazioni predefinite. Per ulteriori informazioni sulla configurazione delle proprietà del master e della replica, consultare la sezione Configurazione delle proprietà del server master o di replica.

    Nota: selezionare un'unità diversa per l'esecuzione dello spool delle proprietà del master ed evitare che la posizione di spool predefinita (C:) riempia il drive locale. (consigliato)

14. Fare clic su Avanti.

    Viene visualizzata la schermata Verifica scenario.

    Il software convalida il nuovo scenario e ne verifica i parametri per assicurare il completamento corretto della replica. Una volta completata la verifica, la schermata viene aperta e mostra eventuali problemi e avvisi. Il software consente di procedere anche in caso di visualizzazione di avvisi. Se necessario, risolvere gli avvisi.

15. Fare clic su Avanti quando tutti gli errori e gli avvisi saranno stati risolti.

    Viene visualizzata la schermata Esecuzione scenario.

16. Selezionare Fine.

Lo scenario CA ARCserve Replication and High Availability è stato creato correttamente. È ora possibile eseguire questo scenario ed eseguire il backup dei file del computer virtuale creati da CA ARCserve D2D.

Importante. Si raccomanda di consultare la console egli eventi per verificare che la sincronizzazione iniziale dei dati sia stata completata. in caso contrario si verificherà un errore del processo di backup.

Considerazioni sull'installazione

Prima di installare CA ARCserve Central Virtual Standby, esaminare le seguenti considerazioni sull'installazione:

- Il pacchetto di installazione di CA ARCserve Central Applications installa un modulo denominato Server CA ARCserve Central Applications. Il server è un modulo comune a tutte le applicazioni. Il modulo contiene il servizio Web, i file binari e le configurazioni che consentono alle applicazioni di comunicare tra loro.

  Durante l'installazione dell'applicazione, il modulo server CA ARCserve Central Applications viene installato prima dei componenti del prodotto. Nel caso in cui fosse necessario applicare una patch all'applicazione, la patch aggiornerà il modulo prima di aggiornare i componenti del prodotto.

- CA ARCserve D2D esegue l'installazione di Virtual Disk Development Kit (VDDK) di VMware su tutti i computer su cui è installato CA ARCserve D2D. Non è necessario scaricare e installare VDDK sui sistemi proxy di Virtual Standby.

  Se si desidera utilizzare una versione diversa di VDDK, scaricare e installare VDDK, quindi modificare il valore del registro di sistema di VDDKDirectory situato in HKEY_LOCAL_MACHINE\SOFTWARE\CA\CA ARCSERVE D2D nella cartella di installazione del nuovo VDDK.

  La directory predefinita per VDDK è la seguente:

  - **Sistema operativo X64**

    `c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit`

    Nota: decomprimere il file VDDK64.zip dalla directory di installazione nella cartella VDDK64.

    Ad esempio: c:\Program Files (x86)\VMware\VMware Virtual Disk Development Kit\VDDK64

  - **Sistema operativo X86**

    `c:\Program Files\VMware\VMware Virtual Disk Development Kit`

- CA ARCserve Central Virtual Standby non supporta la creazione di immagini di dischi virtuali su volumi compressi e volumi crittografati dal file system.

  Nota: questo limite si applica solo ad hypervisor Hyper-V.

- CA ARCserve Central Virtual Standby non supporta la protezione di computer virtuali VMware denominati utilizzando i caratteri Unicode JIS2004.

- CA ARCserve Central Virtual Standby non supporta la protezione di computer virtuali con dischi di dimensioni superiori a due terabyte.

Installazione di CA ARCserve Central Virtual Standby

La procedura guidata di installazione consente all'utente di installare una o più applicazioni di CA ARCserve Central Applications.

Nota: prima di installare l'applicazione, consultare il file delle Note di rilascio e verificare che tutte le attività descritte nella sezioneAttività preliminari siano complete.

Per installare CA ARCserve Central Virtual Standby

1. Scaricare il pacchetto di installazione di CA ARCserve Central Applications sul computer su cui si desidera installare l'applicazione, quindi fare doppio clic sul file di installazione.

   I contenuti del pacchetto di installazione verranno estratti sul computer e verrà visualizzata la finestra di dialogo Componenti richiesti.

2. Fare clic su Installa.

   Nota: la finestra di dialogo Componenti richiesti viene visualizzata solo se il programma di installazione non rileva che i componenti richiesti sono installati sul computer di destinazione.

   Al termine dell'installazione dei componenti richiesti, verrà visualizzata la finestra di dialogo Contratto di licenza.

3. Selezionare le opzioni necessarie, quindi fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Configurazione.

4. Sulla finestra di dialogo Configurazione, completare i seguenti campi:

   - **Componenti** - Specificare le applicazioni che si desidera installare.

     Nota: se l'applicazione viene installata mediante il pacchetto di installazione, è possibile installare più applicazioni simultaneamente.

   - **Posizione** - Accettare la posizione di installazione predefinita o fare clic su Sfogliare per specificare una posizione di installazione alternativa. La directory predefinita è la seguente:

     ```
     C:\Programmi\CA\ARCserve Central Applications
     ```

   - **Informazioni sul disco** - Verificare che il disco rigido disponga dello spazio sufficiente per l'installazione delle applicazioni.

   - **Nome dell'amministratore di Windows** - Specificare il nome utente dell'account di amministratore di Windows utilizzando la seguente sintassi:

     ```
     Dominio\Nome utente
     ```

   - **Password** - Specificare la password per l'account utente.

   - **Specificare il numero di porta** - Specificare il numero di porta da utilizzare per la comunicazione con l'interfaccia utente Web. Si consiglia di accettare il numero di porta predefinito. Il numero predefinito della porta è il seguente:

     ```
     8015
     ```

     Nota: per specificare un numero di porta alternativo, sarà necessario indicare un numero di porta compreso fra 1024 e 65535. Prima di indicare un numero di porta alternativo, verificare che il numero specificato sia libero e disponibile per l'uso. Il programma di installazione, infatti, non consente di installare l'applicazione se la porta selezionata non è disponibile per l'uso.

   - **Usa https per la comunicazione Web -** Specificare l'utilizzo della comunicazione HTTPS per la trasmissione dati. Per impostazione predefinita questa opzione è deselezionata.

     Nota: il protocollo HTTPS (protetto) fornisce un livello di protezione superiore rispetto alla comunicazione HTTP. Il protocollo di comunicazione HTTPS è consigliato se si trasmettono informazioni riservate sulla rete.

- **Consenti al programma di installazione di registrare servizi/programmi di CA ARCserve Central Applications su Windows Firewall come eccezioni** - Verificare che la casella di controllo accanto a questa opzione sia selezionata. Le eccezioni firewall sono necessarie se si desidera configurare e gestire CA ARCserve Central Applications da computer remoti.

  Nota: per gli utenti locali, non è necessario registrare le eccezioni firewall.

Fare clic su Avanti.

Il processo di installazione viene eseguito.

Al completamento del processo di installazione, viene visualizzata la finestra di dialogo Rapporto installazione.

5. La finestra di dialogo Rapporto installazione presenta un riepilogo di installazione. Per verificare la presenza di aggiornamenti per l'applicazione, fare clic su Verifica aggiornamenti e fare clic su Fine.

L'applicazione verrà installata.

Disinstallazione di CA ARCserve Central Virtual Standby

La disinstallazione delle applicazioni può essere effettuata anche da Programmi e funzionalità nel Pannello di controllo di Windows.

Procedere come descritto di seguito:

1. Dal menu Start di Windows, fare clic su Pannello di controllo.

   Verrà visualizzato il Pannello di controllo di Windows.

2. Fare clic sull'elenco a discesa Visualizza quindi su Icone grandi o Icone piccole.

   Le icone del pannello di controllo di Windows verranno visualizzate in un layout griglia.

3. Fare clic su Programmi e funzionalità.

   Verrà visualizzata la finestra Disinstalla o modifica programma.

4. Individuare e fare clic sull'applicazione che si desidera disinstallare.

   Fare clic con il pulsante destro del mouse sull'applicazione, quindi fare clic su Disinstalla dal menu di scelta rapida.

   Seguire le istruzioni visualizzate sullo schermo per completare la disinstallazione.

L'applicazione verrà disinstallata.

Installare CA ARCserve Central Virtual Standby in modalità invisibile all'utente

CA ARCserve Central Applications consente di installare CA ARCserve Central Virtual Standby in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessaria alcuna operazione da parte dell'utente. Di seguito è descritta la procedura per installare l'applicazione utilizzando la riga di comando di Windows.

Per installare CA ARCserve Central Virtual Standby in modalità invisibile all'utente

1. Aprire la riga di comando di Windows nel computer in cui si desidera iniziare il processo di installazione invisibile all'utente.
2. Scaricare il pacchetto di installazione autoestraente di CA ARCserve Central Applications.

   Avviare il processo di installazione invisibile all'utente utilizzando la seguente sintassi della riga di comando:

   ```
   "CA ARCserve Central Applications Setup.exe" /s /v"/q -Path:<INSTALLDIR>
   -Port:<PORT> -U:<UserName> -P:<Password> -Products:<ProductList>"
   ```

   Uso:

   s

   Consente di avviare il pacchetto di file eseguibile in modalità invisibile all'utente.

   v

   Consente di specificare ulteriori opzioni della riga di comando.

   q

   Consente di installare l'applicazione in modalità invisibile all'utente.

   -Percorso:<INSTALLDIR>

   (Facoltativo) Consente di specificare il percorso di destinazione dell'installazione.

   Esempio:

   ```
   -Percorso:C:\Programmi\CA\ARCserve Central Applications
   ```

   Nota: se il valore di INSTALLDIR contiene uno spazio, racchiudere il percorso tra virgolette e barre rovesciate. Inoltre, il percorso non può terminare con una barra rovesciata.

   -Port:<PORTA>

   (Facoltativo) Consente di specificare il numero di porta per la comunicazione.

   Esempio:

   ```
   -Port:8015
   ```

-U:<NomeUtente>

Consente di specificare il nome utente da utilizzare per installare ed eseguire l'applicazione.

Nota: il nome utente deve corrispondere a un account amministrativo o a un account con privilegi amministrativi.

-P:<Password>

Consente di specificare la password per il nome utente.

-Products:<Elenco prodotti>

(Facoltativo) Consente di specificare l'installazione in modalità invisibile all'utente di CA ARCserve Central Applications. Se non si specifica un valore per questo argomento, durante la procedura di installazione invisibile all'utente vengono installati tutti i componenti di CA ARCserve Central Applications.

CA ARCserve Central Host-Based VM Backup

VSPHEREX64

CA ARCserve Central Protection Manager

CMX64

CA ARCserve Central Reporting

REPORTINGX64

CA ARCserve Central Virtual Standby

VCMX64

Tutte le applicazioni CA ARCserve Central Applications

TUTTO

Nota: gli esempi riportati di seguito descrivono la sintassi per eseguire l'installazione di una o più applicazioni CA ARCserve Central Applications in modalità invisibile all'utente:

```
-Products:CMX64
-Products:CMX64,VCMX64
-Products:CMX64,VCMX64,REPORTINGX64
-Products:ALL
```

L'applicazione verrà installata in modalità invisibile all'utente.

Disinstallare CA ARCserve Central Virtual Standby in modalità invisibile all'utente

CA ARCserve Central Applications consente di disinstallare CA ARCserve Central Virtual Standby in modalità invisibile all'utente. Se si utilizza l'installazione invisibile all'utente, non sarà necessaria alcuna operazione da parte dell'utente. Di seguito è descritta la procedura per disinstallare l'applicazione utilizzando la riga di comando di Windows.

Procedere come descritto di seguito:

1. Accedere al computer da cui si desidera disinstallare l'applicazione.

   Nota: è necessario accedere con un account amministrativo o un account con privilegi amministrativi.

2. Aprire la riga di comando di Windows ed eseguire il seguente comando per avviare il processo di disinstallazione invisibile all'utente:

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ProductCode>
   ```

   Oppure

   ```
   <INSTALLDIR>%\Setup\uninstall.exe /q /p <ALL>
   ```

   Esempio: la sintassi seguente consente di disinstallare CA ARCserve Central Virtual Standby in modalità invisibile all'utente.

   ```
   "%Programmi%\CA\ARCserve Central Applications\Setup\uninstall.exe" /q /p
   {CAED4835-964B-484B-A395-E2DF12E6F73D}
   ```

Uso:

<INSTALLDIR>

Consente di specificare la directory in cui è installata l'applicazione.

Nota: eseguire la sintassi corrispondente all'architettura del sistema operativo del computer.

<CodiceProdotto>

Consente di specificare l'applicazione da disinstallare in modalità invisibile all'utente.

Nota: la procedura di disinstallazione invisibile all'utente consente di installare una o più applicazioni di CA ARCserve Central Applications. Utilizzare i seguenti codici di prodotto per disinstallare CA ARCserve Central Applications in modalità invisibile all'utente:

CA ARCserve Central Host-Based VM Backup

{CAED49D3-0D3C-4C59-9D99-33AFAF0C7126}

CA ARCserve Central Protection Manager

{CAED05FE-D895-4FD5-B964-001928BD2D62}

CA ARCserve Central Reporting

{CAED8DA9-D9A8-4F63-8689-B34DEEEEC542}

CA ARCserve Central Virtual Standby

{CAED4835-964B-484B-A395-E2DF12E6F73D}

L'applicazione verrà disinstallata in modalità invisibile all'utente.

Capitolo 3: Configurazione di criteri Virtual Standby

Questa sezione contiene i seguenti argomenti:

Rilevamento dei nodi

CA ARCserve Central Virtual Standby consente di utilizzare diversi metodi per eseguire il rilevamento o l'aggiunta dei nodi:

Criterio locale:

- Aggiunta di nodi per indirizzo IP o nome nodo (a pagina 33)
- Aggiunta di nodi da un file (a pagina 34)
- Aggiunta di nodi dai server CA ARCserve Central Host-Based VM Backup (a pagina 36)

Criterio remoto:

- Importazione dei nodi da CA ARCserve Replication and High Availability (a pagina 39)

Aggiunta di nodi per indirizzo IP o nome nodo

Virtual Standby consente di aggiungere nodi in base all'indirizzo IP o al nome del nodo. Aggiungere i nodi di origine di CA ARCserve D2D che si desidera proteggere.

Nota: questa opzione si applica unicamente ai criteri locali di Virtual Standby.

Per aggiungere nodi per indirizzo IP o nome nodo

1. Dalla pagina principale, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra degli strumenti Nodo, fare clic su clic Aggiungi, quindi selezionare Aggiungi nodo per IP/Nome dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiungi nodo per IP/Nome.

3. Completare i seguenti campi:
   - **IP/Nome nodo** - Consente di specificare l'indirizzo IP o il nome del nodo.
   - **Descrizione** - Consente di specificare una descrizione per il nodo.
   - **Nome utente** - Consente di specificare il nome utente richiesto per l'accesso al nodo.
   - **Password** - Consente di specificare la password richiesta per l'accesso al nodo.

   Fare clic su OK.
4. (Facoltativo) Se il nodo aggiunto non compare nell'elenco dei nodi, fare clic su Aggiorna nella barra degli strumenti.

La finestra di dialogo Aggiungi nodo per IP/Nome verrà chiusa e il nodo verrà aggiunto.

Importare nodi da un file

CA ARCserve Central Virtual Standby consente di importare più nodi da un file. È possibile importare nodi da un file di testo di valori delimitati da virgole (.txt) o da un foglio di calcolo (.CSV).

L'applicazione consente di importare fino a 100 nodi da un file. Se il file contiene più di 100 nodi, l'applicazione importerà solamente i primi 100 nodi. Se si desidera aggiungere più di 100 nodi, importare i primi 100 tramite un file, quindi aggiungere i nodi restanti manualmente

Nota: questa opzione si applica unicamente ai criteri locali di Virtual Standby. Per informazioni su come aggiungere nodi manualmente, consultare la sezione Aggiunta di nodi per indirizzo IP o nome nodo (a pagina 33).

Per eseguire l'importazione dei nodi da un file

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.
2. Dalla barra degli strumenti Nodo, fare clic su Aggiungi, quindi selezionare Importa nodi da file nel menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Seleziona nodi.
3. Fare clic su Sfoglia per specificare il file contenente i nodi da importare.

   Nota: è possibile specificare file di testo di valori delimitati da virgole (.txt) o da un foglio di calcolo (.CSV).

   Fare clic su Carica.

   I nomi dei nodi e i nomi utenti corrispondenti verranno visualizzati nella finestra di dialogo.

4. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Credenziali nodo.

   Se il nome utente e la password immessi sono corretti, verrà visualizzato un segno di spunta verde nel campo Verificato. Se il nome utente e la password immessi non sono corretti, verrà visualizzato un punto esclamativo di colore rosso nel campo Verificato.

5. Eseguire una delle seguenti operazioni:

   - Per aggiungere i nodi, verificare che i nomi utenti e le password siano corretti. Per modificare le credenziali per un nodo specifico, fare clic sul campo Nome nodo.

     Verrà visualizzata la finestra di dialogo Convalida credenziali.

     Compilare i campi obbligatori nella finestra di dialogo Convalida credenziali e fare clic su OK.

   - Per applicare un nome utente e una password globale a tutti i nodi, completare i campi Nome utente e Password, quindi fare clic su Applica ai nodi selezionati.

     Il nome utente globale e la password globale verrà applicato a tutti i nodi.

   Fare clic su Fine.

I nodi verranno aggiunti.

Aggiunta di nodi dai server CA ARCserve Central Host-Based VM Backup

CA ARCserve Central Host-Based VM Backup è un'applicazione che consente di eseguire il backup di computer virtuali utilizzando un'istanza di CA ARCserve D2D installata su un server proxy. CA ARCserve Central Virtual Standby consente di aggiungere i nodi protetti dai server CA ARCserve Central Host-Based VM Backup in modo che sia possibile creare le snapshot del punto di ripristino per i nodi. È necessario che i computer virtuali dispongano di criteri CA ARCserve D2D assegnati mediante CA ARCserve Central Host-Based VM Backup.

Tenere presenti le seguenti considerazioni:

- Questa opzione si applica unicamente ai criteri locali di Virtual Standby.
- CA ARCserve Central Virtual Standby consente di utilizzare diversi metodi per l'aggiunta dei nodi:
  - Aggiunta manuale dei nodi
  - Aggiunta di nodi da un file di testo
  - Aggiunta di nodi dai server CA ARCserve Central Host-Based VM Backup

  CA ARCserve Central Virtual Standby consente di applicare direttamente i criteri ai nodi, mentre con CA ARCserve Central Host-Based VM Backup i criteri vengono applicati ai server proxy di backup. Questo comportamento persiste dopo l'aggiunta di nodi dai server CA ARCserve Central Host-Based VM Backup.

  Nota: per informazioni sull'assegnazione di criteri di CA ARCserve D2D ai nodi di computer virtuali, consultare la *Guida per l'utente di CA ARCserve Central Host-Based VM Backup*.
- Virtual Standby non è in grado di attivare le snapshot del punto di ripristino per i nodi aggiunti automaticamente dai server CA ARCserve Central Host-Based VM Backup. È invece possibile attivare le snapshot del punto di ripristino per i nodi aggiunti manualmente dai server CA ARCserve Central Host-Based VM Backup.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.
2. Dalla categoria Nodo, fare clic su Aggiungi, quindi selezionare Aggiungi computer virtuale da un server CA ARCserve Central Host-Based VM Backup nel menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiungi computer virtuale da un server CA ARCserve Central Host-Based VM Backup.

3. Completare i seguenti campi della finestra di dialogo Aggiungi computer virtuale dal server CA ARCserve Central Host-Based VM Backup:

   - **Nome computer -** Consente di specificare l'indirizzo IP o il nome host del server CA ARCserve Central Host-Based VM Backup.
   - **Nome utente -** Consente di specificare il nome utente per l'accesso al server CA ARCserve Central Host-Based VM Backup.
   - **Password -** Consente di specificare la password per l'accesso al server CA ARCserve Central Host-Based VM Backup.
   - **Porta -** Consente di specificare il numero di porta che dovrà essere utilizzato dall'applicazione per comunicare con il server CA ARCserve Central Host-Based VM Backup.
   - **Usa HTTPS** - Consente di indicare se si desidera utilizzare la comunicazione HTTPS protetta.

   Fare clic su OK.

   Si verifica quanto segue:

   - Se si tratta della prima importazione dei nodi dal sistema server ESX, Virtual Standby importa tutti i computer virtuali contenenti un'assegnazione di criterio CA ARCserve Central Host-Based VM Backup. Una volta completato il processo di importazione, è possibile verificare i nodi nella schermata Nodi.
   - Se non si tratta della prima importazione dei nodi dal sistema server ESX, la finestra di dialogo Aggiungi computer virtuale da un server CA ARCserve Central Host-Based VM Backup mostra un elenco dei nodi importati precedentemente. Verrà visualizzata una finestra di dialogo che richiede all'utente se desidera sovrascrivere le informazioni relative ai nodi importati precedentemente.
   - Se l'applicazione non è in grado di rilevare nuovi nodi, la finestra di dialogo Aggiungi computer virtuale da un server CA ARCserve Central Host-Based VM Backup verrà chiusa. Un messaggio informerà l'utente che non è stato importato alcun nodo.

4. Effettuare una delle seguenti operazioni:

   - **Per aggiungere i nodi appena rilevati e sovrascrivere i nodi rilevati in precedenza:** selezionare la casella di controllo accanto ai nodi importati e fare clic su OK.

     I nodi appena rilevati verranno aggiunti e i nodi rilevati in precedenza verranno sovrascritti. L'applicazione sovrascrive solo lo stato e le credenziali corrispondenti ai nodi rilevati in precedenza.

   - **Per aggiungere solo i nodi appena rilevati (senza eseguire l'importazione e la sovrascrittura dei noti precedenti):** Non selezionare la casella di controllo accanto ai nodi importati precedentemente e fare clic su OK.

     Verranno aggiunti solo i nodi appena rilevati. I nodi rilevati in precedenza non verranno sovrascritti.

   - **Per uscire senza aggiungere i nodi appena rilevati e i nodi rilevati in precedenza:** fare clic su Annulla.

     Non verrà aggiunto alcun nodo.

5. (Facoltativo) Fare clic sul pulsante Aggiorna sulla barra degli strumenti per verificare che tutti i nodi appena aggiunti vengano visualizzati nell'elenco di nodi.

I nodi verranno aggiunti.

Nota: quando le informazioni di CA ARCserve D2D vengono aggiornate sul server CA ARCserve Central Host-Based VM Backup, il server comunica automaticamente a CA ARCserve Central Virtual Standby di eseguire l'importazione dei computer virtuali da CA ARCserve Central Host-Based VM Backup e distribuire nuovamente i criteri. Se CA ARCserve Central Virtual Standby non è disponibile, è possibile eseguire l'importazione manuale dei computer virtuali da CA ARCserve Central Host-Based VM Backup.

Importazione dei nodi da CA ARCserve Replication

CA ARCserve Central Virtual Standby consente di importare uno o più nodi da CA ARCserve Replication and High Availability. Per eseguire l'importazione dei nodi, specificare le informazioni nella gestione della replica in cui si desidera importare i nodi.

Nota: questa opzione si applica unicamente ai criteri remoti di Virtual Standby (a pagina 47). Prima di importare i nodi, è necessario creare uno scenario CA ARCserve Replication and High Availability per un criterio remoto di Virtual Stansdby (a pagina 17).

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra degli strumenti Nodo, fare clic su Aggiungi, quindi selezionare Importa nodi da CA ARCserve Replication dal menu di scelta rapida.

   Viene visualizzata la finestra di dialogo Importa nodi da CA ARCserve Replication.

3. Specificare il nome host di gestione, la porta, il protocollo, il nome utente e la password per la replica contenente i nodi che si desidera importare.

   Fare clic su Connetti.

   Nella finestra di dialogo verranno visualizzati i nomi di nodo, il nome dello scenario, il convertitore, la posizione di backup e lo stato della configurazione.

4. Fare clic su Importa.

I nodi vengono importati e visualizzati nella schermata Nodo.

Configurazione di convertitori remoti

CA ARCserve Central Virtual Standby consente di eseguire la conversione dei punti di ripristino di CA ARCserve D2D protetti da CA ARCserve Replication and High Availability e registrati automaticamente con Microsoft Hyper-V, VMware vCenter o ESXi.

Una volta completata l'importazione dei nodi da CA ARCserve Replication and High Availability a CA ARCserve Central Applications, sarà possibile eseguirne la conversione. La conversione avviene dalla cartella di replica di CA ARCserve Replication and High Availability.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo Tutti i nodi oppure sul nome del gruppo contenente i nodi che si desidera convertire.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Fare clic sul convertitore che si desidera configurare nella colonna Convertitore.

   Viene visualizzata la finestra di dialogo Configurazione dei convertitori remoti.

4. Specificare la porta, il protocollo, il nome utente e la password per il convertitore selezionato e fare clic su Aggiorna per salvare le informazioni.

La configurazione del convertitore viene completata.

Creazione dei criteri CA ARCserve Central Virtual Standby

Virtual Standby consente di creare due tipi di criteri per definire i criteri di conversione personalizzati assegnati ai nodi di CA ARCserve D2D. I due tipi di criteri sono:

- Criterio locale di Virtual Standby (a pagina 40)
- Criterio remoto di Virtual Standby (a pagina 47)

Nota: per la creazione di criteri è necessario che CA ARCserve D2D sia installato sul server di monitoraggio.

Creazione dei criteri locali di Virtual Standby

Virtual Standby consente di creare criteri locali di standby virtuale per definire i criteri di conversione personalizzati assegnati ai nodi di CA ARCserve D2D.

Nota: per la creazione di criteri è necessario che CA ARCserve D2D sia installato sul server di monitoraggio.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby, quindi aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Criteri.

   Verrà visualizzata la finestra dei criteri.

2. Fare clic su Nuovo, quindi selezionare Nuovo criterio locale di Virtual Standby dal menu di scelta rapida.

   Viene visualizzata la finestra di dialogo Creazione del criterio locale di Virtual Standby.

3. Nel campo Nome criterio, immettere il nome del criterio.

   Fare clic sulla scheda Virtual Standby.

   Verranno visualizzate le opzioni del server di virtualizzazione, del computer virtuale e delle impostazioni di sostituzione.

4. Fare clic su Server di virtualizzazione.

   Verranno visualizzate le opzioni del server di virtualizzazione.

5. Compilare le seguenti opzioni del server di virtualizzazione:

   Sistemi VMware

   - **Tipo di virtualizzazione** - Fare clic su VMware.
   - **Host ESX/vCenter -** Consente di specificare il nome host del sistema ESX o vCenter Server.
   - **Nome utente** - Consente di specificare il nome utente per l'accesso al sistema VMware.

     Nota: l'account specificato deve essere un account amministrativo o un account con privilegi di amministratore per il sistema ESX o vCenter Server.
   - **Password** - Specificare la password associata al nome utente per l'accesso al sistema VMware.
   - **Protocollo** - Specificare HTTP o HTTPS come il protocollo da utilizzare per la comunicazione tra il nodo di origine di CA ARCserve D2D e il server di monitoraggio.
   - **Porta -** Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server di origine e il server di monitoraggio.
   - **Nodo ESX** - I valori in questo campo variano in base al valore specificato nel campo Host ESX/vCenter.
     - **Sistemi server ESX** - Quando viene specificato un sistema server ESX nel campo Host ESX/vCenter, questo campo visualizza il nome host del sistema server ESX.
     - **Sistemi server vCenter** - Quando viene specificato un sistema server vCenter nel campo Host ESX/vCenter, questo campo consente specificare (da un elenco a discesa) il sistema server ESX da associare a questo criterio.
   - **Server di monitoraggio** - Specificare il nome host del server che dovrà monitorare lo stato del server di origine.

     Nota: il server di monitoraggio può essere qualsiasi computer fisico o virtuale purché tale server non funzioni come server proxy per un'implementazione di CA ARCserve Central Host-Based VM Backup.
   - **Nome utente** - Specificare il nome utente per l'accesso al sistema di monitoraggio.
   - **Password** - Specificare la password associata al nome utente per l'accesso al sistema di monitoraggio.
   - **Protocollo** - Specificare HTTP o HTTPS come il protocollo da utilizzare per la comunicazione tra il server CA ARCserve Central Virtual Standby e il Sistema Server ESX (server di monitoraggio).

- **Porta** - Specificare la porta che si desidera utilizzare per il trasferimento di dati tra il server CA ARCserve Central Virtual Standby e il Sistema Server ESX (server di monitoraggio).
- **Usa server di monitoraggio come proxy per il trasferimento dei dati** - Specificare questa opzione per consentire al server di monitoraggio di copiare i dati di conversione dal nodo di origine di CA ARCserve D2D all'archivio dati del server ESX. Abilitando questa opzione, Virtual Standby trasferisce i dati di conversione dal nodo di origine all'archivio dati del server ESX mediante comunicazione Fibre Channel, più veloce della comunicazione LAN per il trasferimento dei dati.

  Nota: l'opzione Usa server di monitoraggio come proxy per il trasferimento dei dati è abilitata per impostazione predefinita. È possibile disattivare questa opzione per consentire al server di origine CA ARCserve D2D di copiare i dati di conversione direttamente nell'archivio dati del sistema server ESX.

Sistemi Hyper-V

- **Tipo di virtualizzazione** - Fare clic su Hyper-V.
- **Nome host Hyper-V** - Specificare il nome host del sistema Hyper-V.
- **Nome utente** - Consente di specificare il nome utente per l'accesso al sistema Hyper-V.

  Nota: l'account specificato deve essere un account amministrativo o un account con privilegi di amministratore sul sistema Hyper-V.
- **Password** - Specificare la password associata al nome utente per l'accesso al sistema Hyper-V.
- **Porta -** Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server di origine e il server di monitoraggio.
- **Nome utente** - Specificare il nome utente per l'accesso al sistema di monitoraggio.
- **Password** - Specificare la password associata al nome utente per l'accesso al sistema di monitoraggio.
- **Protocollo** - Specificare HTTP o HTTPS come il protocollo da utilizzare per la comunicazione tra il server CA ARCserve Central Virtual Standby e il Sistema Server Hyper-V (server di monitoraggio).
- **Porta** - Specificare la porta che si desidera utilizzare per il trasferimento di dati tra il server CA ARCserve Central Virtual Standby e il Sistema Server Hyper-V (server di monitoraggio).

Fare clic su Computer virtuale.

Verranno visualizzate le opzioni del computer virtuale.

6. Compilare le seguenti opzioni del computer virtuale:

   Sistemi VMware

   Per sistemi VMware, applicare le opzioni seguenti al computer virtuale:

   - **Prefisso nome del computer virtuale -** Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema server ESX.

     Valore predefinito: CAVM_

   - **Pool di risorse del computer virtuale** - Specificare il nome del pool di risorse in cui si desidera raggruppare il computer virtuale di standby.

   - **Conteggio CPU** - Specifica il numero minimo e massimo di CPU supportato dal computer virtuale di standby.

   - **Memoria** - Specifica la quantità totale di RAM in MB da allocare per il computer virtuale di standby.

     Nota: il valore di RAM specificato deve essere un multiplo di due.

   - **Archivio dati del computer virtuale** - Specificare la posizione in cui si desidera archiviare i dati di conversione.

     - **Specifica un archivio dati per tutti i dischi virtuali** - Consente all'applicazione di copiare tutti i dischi correlati al computer virtuale in un unico archivio dati.

     - **Specifica un archivio dati per ogni disco virtuale** - Consente all'applicazione di copiare le informazioni relative al disco del computer virtuale nell'archivio dati corrispondente.

   - **Rete del computer virtuale** - Consente di definire le NIC, le reti virtuali e i percorsi che il sistema server ESX dovrà utilizzare per comunicare con i computer virtuali.

     - **Specifica un tipo di scheda di rete per ciascuna NIC e connetti la scheda di rete alla seguente rete virtuale** - Consente di definire il mapping della NIC virtuale alla rete virtuale. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.

     - **Specifica un tipo di scheda di rete e una rete virtuale per ciascuna NIC** - Consente di definire il nome della rete virtuale da utilizzare per la comunicazione della scheda NIC.

Sistemi Hyper-V

Per sistemi Hyper-V, applicare le opzioni seguenti al computer virtuale:

- **Impostazioni di base del computer virtuale** - Completare le seguenti impostazioni di base del computer virtuale:
  - **Prefisso nome del computer virtuale** - Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema Hyper-V.

    Valore predefinito: CAVM_

    Conteggio CPU - Specificare il numero minimo e il numero massimo di CPU supportato dal sistema virtuale in standby.
  - **Memoria** - Specificare la quantità totale di RAM in MB da allocare per il computer virtuale di standby.

    Nota: il valore di RAM specificato deve essere un multiplo di quattro.
- **Percorso del computer virtuale** - Specificare una della seguenti opzioni:
  - **Specifica un percorso per tutti i dischi virtuali** - Specificare la posizione in cui si desidera archiviare i dati di conversione sul server Hyper-V.
  - **Specifica un percorso per ogni disco virtuale** - Specificare la posizione in cui si desidera archiviare i dati di conversione per ciascun disco virtuale sul server Hyper-V.

  Nota: CA ARCserve Central Virtual Standby non supporta la creazione di immagini di dischi virtuali (file VHD) su volumi compressi e volumi crittografati dal file system. Se il percorso specificato si trova su volumi Hyper-V compressi o crittografati, Virtual Standby impedisce la creazione del criterio.
- **Rete del computer virtuale** - Consente di definire le NIC, le reti virtuali e i percorsi che il server Hyper-V dovrà utilizzare per comunicare con i computer virtuali. Specificare una delle opzioni seguenti e completare i campi obbligatori.
  - **Specifica un tipo di scheda di rete per ciascuna NIC e connetti la scheda di rete alla rete virtuale seguente** - Consente di definire il mapping della NIC virtuale alla rete virtuale. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.
  - **Specifica un tipo di scheda di rete e una rete virtuale per ciascuna NIC** - Consente di definire il nome della rete virtuale da utilizzare per la comunicazione della scheda NIC.

Fare clic su Impostazioni di sostituzione.

Verranno visualizzate le opzioni delle impostazioni di sostituzione.

7. Compilare le seguenti opzioni:

   Recupero:

   Selezionare uno dei metodi seguenti:

   - **Avvia il computer virtuale manualmente** - Consente di attivare i computer virtuali ed eseguirne il provisioning manualmente quando si verificano errori sul server di origine o la comunicazione viene interrotta. Specificare questa opzione se si preferisce analizzare la causa dell'errore prima di eseguire il provisioning dei computer virtuali e di consentire ai server di funzionare come server di origine.
   - **Avvia il computer virtuale automaticamente** - Consente di attivare i computer virtuali ed eseguirne il provisioning automaticamente quando si verificano errori sul server di origine o la comunicazione viene interrotta. Specificare questa opzione se si desidera consentire ai computer virtuali di funzionare come server di origine subito dopo un errore o un problema di comunicazione dei server di origine.

   Nota: l'opzione selezionata per impostazione predefinita Avvia il computer virtuale manualmente.

   Proprietà heartbeat:

   - **Timeout** - Specifica la durata dell'attesa di un heartbeat da parte del server di monitoraggio prima di attivare la snapshot di un punto di ripristino.
   - **Frequenza** - Specifica la frequenza con cui il server di origine comunica gli heartbeat al server di monitoraggio.

     Esempio: il valore di timeout specificato è 60. Il valore di frequenza specificato è 10. Il server di origine comunicherà gli heartbeat ogni 10 secondi. Se il server di monitoraggio non rileva un heartbeat entro 60 secondi dell'ultimo heartbeat rilevato, attiva un computer virtuale utilizzando la snapshot del punto di ripristino più recente.

   Fare clic sulla scheda Preferenze.

   Verrà visualizzata la finestra delle opzioni degli avvisi di posta elettronica.

8. Compilare le seguenti opzioni:

   - **Heartbeat mancante per il computer di origine** - Virtual Standby invia notifiche di avviso quando il server di monitoraggio non rileva un heartbeat nel server di origine.
   - **Computer virtuale attivo per il computer di origine configurato con attivazione automatica** - Virtual Standby invia notifiche di avviso quando viene attivato un computer virtuale configurato per l'attivazione automatica nel caso in cui l'heartbeat non venga rilevato.
   - **Heartbeat mancante per il computer di origine configurato con attivazione manuale** - Virtual Standby invia notifiche di avviso quando non viene rilevato l'heartbeat di un server di origine non configurato per l'attivazione automatica.

- **Spazio di archiviazione disponibile sul computer virtuale inferiore a** - Virtual Standby invia notifiche di avviso quando viene rilevato spazio su disco insufficiente sul percorso dell'hypervisor definito. Ciò si verifica quando la quantità di spazio disponibile su disco è inferiore alla soglia definita dall'utente. La soglia può essere rappresentata da un valore assoluto (MB) o da una percentuale della capacità del volume.
- **Errori/Arresto anomalo dello standby virtuale** - Virtual Standby invia notifiche di avviso quando si verifica un errore durante il processo di conversione.
- **Virtual Standby eseguito correttamente** - Virtual Standby invia notifiche di avviso quando rileva che un computer virtuale è stato attivato correttamente.
- **Hypervisor non raggiungibile** - Virtual Standby invia notifiche di avviso quando vengono rilevati errori di comunicazione con il sistema ESX Server o Hyper-V.
- **Errore di licenza** - Virtual Standby invia notifiche di avviso quando vengono rilevati problemi di licenza su server Virtual Standby, su server di origine e su server di monitoraggio.
- **Errore di avvio di Virtual Standby dalla snapshot del punto di ripristino** - Se è stata specificata l'opzione Avvia il computer virtuale automaticamente, Virtual Standby invia notifiche di avviso in caso di rilevamento di computer virtuali non avviati automaticamente.

Fare clic su Salva.

Il criterio viene salvato.

Creazione dei criteri remoti di Virtual Standby

Virtual Standby consente di creare criteri remoti di standby virtuale per definire criteri di conversione personalizzati da assegnare ai nodi da CA ARCserve Replication and High Availability.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby e aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Criteri.

   Verrà visualizzata la finestra dei criteri.

2. Fare clic su Nuovo, quindi selezionare Nuovo criterio remoto di Virtual Standby dal menu di scelta rapida.

   Viene visualizzata la finestra di dialogo Creazione dei criteri remoti di Virtual Standby.

3. Nel campo Nome criterio, immettere il nome del criterio.

   Fare clic sulla scheda Virtual Standby.

   Vengono visualizzate le opzioni del server di virtualizzazione e del computer virtuale.

4. Fare clic su Server di virtualizzazione.

   Verranno visualizzate le opzioni del server di virtualizzazione.

5. Compilare le seguenti opzioni del server di virtualizzazione:

   Sistemi VMware:

   - **Tipo di virtualizzazione** - Fare clic su VMware.
   - **Host ESX/vCenter -** Consente di specificare il nome host del sistema ESX o vCenter Server.
   - **Nome utente** - Consente di specificare il nome utente per l'accesso al sistema VMware.

     Nota: l'account specificato deve essere un account amministrativo o un account con privilegi di amministratore per il sistema ESX o vCenter Server.
   - **Password** - Specificare la password associata al nome utente per l'accesso al sistema VMware.
   - **Protocollo** - Specificare HTTP o HTTPS come il protocollo da utilizzare per la comunicazione tra il nodo di origine di CA ARCserve D2D e il server di monitoraggio.
   - **Porta -** Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server di origine e il server di monitoraggio.
   - **Nodo ESX** - I valori in questo campo variano in base al valore specificato nel campo Host ESX/vCenter.
     - **Sistemi server ESX** - Quando viene specificato un sistema server ESX nel campo Host ESX/vCenter, questo campo visualizza il nome host del sistema server ESX.
     - **Sistemi server vCenter** - Quando viene specificato un sistema server vCenter nel campo Host ESX/vCenter, questo campo consente specificare (da un elenco a discesa) il sistema server ESX da associare a questo criterio.

Sistemi Hyper-V

- **Tipo di virtualizzazione** - Fare clic su Hyper-V.
- **Nome host Hyper-V** - Specificare il nome host del sistema Hyper-V.
- **Nome utente** - Consente di specificare il nome utente per l'accesso al sistema Hyper-V.

  Nota: l'account specificato deve essere un account amministrativo o un account con privilegi di amministratore sul sistema Hyper-V.
- **Password** - Specificare la password associata al nome utente per l'accesso al sistema Hyper-V.
- **Protocollo** - Specificare HTTP o HTTPS come il protocollo da utilizzare per la comunicazione tra il nodo di origine di CA ARCserve D2D e il server di monitoraggio.
- **Porta -** Specificare la porta che si desidera utilizzare per il trasferimento dei dati tra il server di origine e il server di monitoraggio.

Fare clic su Computer virtuale.

Verranno visualizzate le opzioni del computer virtuale.

6. Compilare le seguenti opzioni del computer virtuale:

   Sistemi VMware

   Per sistemi VMware, applicare le opzioni seguenti al computer virtuale:

   - **Prefisso nome del computer virtuale -** Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema server ESX.

     Valore predefinito: CAVM_

   - **Pool di risorse del computer virtuale** - Specificare il nome del pool di risorse in cui si desidera raggruppare il computer virtuale di standby.

   - **Conteggio CPU** - Specifica il numero minimo e massimo di CPU supportato dal computer virtuale di standby.

   - **Memoria** - Specifica la quantità totale di RAM in MB da allocare per il computer virtuale di standby.

     Nota: il valore di RAM specificato deve essere un multiplo di due.

   - **Archivio dati del computer virtuale** - Specificare la posizione in cui si desidera archiviare i dati di conversione.

     - **Specifica un archivio dati per tutti i dischi virtuali** - Consente all'applicazione di copiare tutti i dischi correlati al computer virtuale in un unico archivio dati.

     - **Specifica un archivio dati per ogni disco virtuale** - Consente all'applicazione di copiare le informazioni relative al disco del computer virtuale nell'archivio dati corrispondente.

   - **Rete del computer virtuale** - Consente di definire le NIC, le reti virtuali e i percorsi che il sistema server ESX dovrà utilizzare per comunicare con i computer virtuali.

     - **Specifica un tipo di scheda di rete per ciascuna NIC e connetti la scheda di rete alla seguente rete virtuale** - Consente di definire il mapping della NIC virtuale alla rete virtuale. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.

     - **Specifica un tipo di scheda di rete e una rete virtuale per ciascuna NIC** - Consente di definire il nome della rete virtuale da utilizzare per la comunicazione della scheda NIC.

Sistemi Hyper-V

Per sistemi Hyper-V, applicare le opzioni seguenti al computer virtuale:

- **Impostazioni di base del computer virtuale** - Completare le seguenti impostazioni di base del computer virtuale:
  - **Prefisso nome del computer virtuale** - Specificare il prefisso che si desidera aggiungere al nome visualizzato per il computer virtuale sul sistema Hyper-V.

    Valore predefinito: CAVM_

    Conteggio CPU - Specificare il numero minimo e il numero massimo di CPU supportato dal sistema virtuale in standby.
  - **Memoria** - Specificare la quantità totale di RAM in MB da allocare per il computer virtuale di standby.

    Nota: il valore di RAM specificato deve essere un multiplo di quattro.
- **Percorso del computer virtuale** - Specificare una della seguenti opzioni:
  - **Specifica un percorso per tutti i dischi virtuali** - Specificare la posizione in cui si desidera archiviare i dati di conversione sul server Hyper-V.
  - **Specifica un percorso per ogni disco virtuale** - Specificare la posizione in cui si desidera archiviare i dati di conversione per ciascun disco virtuale sul server Hyper-V.

  Nota: CA ARCserve Central Virtual Standby non supporta la creazione di immagini di dischi virtuali (file VHD) su volumi compressi e volumi crittografati dal file system. Se il percorso specificato si trova su volumi Hyper-V compressi o crittografati, Virtual Standby impedisce la creazione del criterio.
- **Rete del computer virtuale** - Consente di definire le NIC, le reti virtuali e i percorsi che il server Hyper-V dovrà utilizzare per comunicare con i computer virtuali. Specificare una delle opzioni seguenti e completare i campi obbligatori.
  - **Specifica un tipo di scheda di rete per ciascuna NIC e connetti la scheda di rete alla rete virtuale seguente** - Consente di definire il mapping della NIC virtuale alla rete virtuale. Specificare questa opzione quando il computer virtuale contiene NIC virtuali e una rete virtuale.
  - **Specifica un tipo di scheda di rete e una rete virtuale per ciascuna NIC** - Consente di definire il nome della rete virtuale da utilizzare per la comunicazione della scheda NIC.

Fare clic sulla scheda Preferenze.

Verrà visualizzata la finestra delle opzioni degli avvisi di posta elettronica.

7. Compilare le seguenti opzioni:

   - **Spazio di archiviazione disponibile sul computer virtuale inferiore a** - Virtual Standby invia notifiche di avviso quando viene rilevato spazio su disco insufficiente sul percorso dell'hypervisor definito. Ciò si verifica quando la quantità di spazio disponibile su disco è inferiore alla soglia definita dall'utente. La soglia può essere rappresentata da un valore assoluto (MB) o da una percentuale della capacità del volume.
   - **Errori/Arresto anomalo dello standby virtuale** - Virtual Standby invia notifiche di avviso quando si verifica un errore durante il processo di conversione.
   - **Virtual Standby eseguito correttamente** - Virtual Standby invia notifiche di avviso quando rileva che un computer virtuale è stato attivato correttamente.
   - **Hypervisor non raggiungibile** - Virtual Standby invia notifiche di avviso quando vengono rilevati errori di comunicazione con il sistema ESX Server o Hyper-V.
   - **Errore di licenza** - Virtual Standby invia notifiche di avviso quando vengono rilevati problemi di licenza su server Virtual Standby, su server di origine e su server di monitoraggio.
   - **Errore di avvio di Virtual Standby dalla snapshot del punto di ripristino** - Se è stata specificata l'opzione Avvia il computer virtuale automaticamente, Virtual Standby invia notifiche di avviso in caso di rilevamento di computer virtuali non avviati automaticamente.

   Fare clic su Salva.

Il criterio viene salvato.

Assegnazione e annullamento dell'assegnazione di nodi ai criteri

Per creare le snapshot del punto di ripristino, assegnare criteri di conversione di standby virtuale ai nodi CA ARCserve D2D che si desidera proteggere.

Virtual Standby consente di annullare l'assegnazione dei nodi dai criteri. Virtual Standby non consente di assegnare più criteri ai nodi. Se si desidera assegnare i nodi a nuovi criteri, è necessario annullare l'assegnazione del criterio corrente ai nodi prima di poter assegnare un nuovo criterio.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby e aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Criteri per visualizzare la schermata corrispondente.

2. Dall'elenco Criteri, fare clic sul criterio che si desidera assegnare ai nodi o di cui si desidera annullare l'assegnazione.

   Le informazioni dettagliate relative al criterio specificate verranno visualizzate nelle schede Dettagli criterio e Assegnazione criterio.

3. Fare clic sulla scheda Dettagli criterio per visualizzare informazioni dettagliate relative al criterio.

   (Facoltativo) Fare clic su Modifica della barra degli strumenti per modificare le impostazioni correnti per il criterio.

   Nota: per ulteriori informazioni, consultare la sezione Modifica dei criteri.

4. Fare clic sulla scheda Assegnazione criterio.

   Fare clic su Assegnazione e annullamento assegnazione della scheda Assegnazione criterio.

   Verrà visualizzata la finestra di dialogo Assegna/Annulla assegnazione criterio.

5. Specificare i campi seguenti nella finestra di dialogo Assegnazione/Annullamento assegnazione criterio:

   - **Gruppo:** selezionare il nome del gruppo contenente i criteri da assegnare.
   - **Filtro Nome nodo:** consente di filtrare i nodi disponibili in base a un criterio comune.

   Nota: il campo Filtro supporta l'uso di caratteri jolly.

   Esempi:

   - Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc.
   - *.123 consente di filtrare tutti i nodi il cui indirizzo IP contiene ".123".

   Nota: per annullare tutti i risultati del filtro, fare clic su X nel campo Filtro.

6. Effettuare una delle seguenti operazioni:

   - **Assegnazione di un nodo:** dall'elenco Nodi disponibili, individuare il nodo che si desidera assegnare al criterio.

     Fare clic sulla freccia destra singola.

     Il nodo verrà spostato dall'elenco Nodi disponibili all'elenco Nodi selezionati.

   - **Assegnazione di nodi:** dall'elenco Nodi disponibili, fare clic sulla freccia destra doppia.

     Tutti i nodi vengono spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati.

   - **Annullamento dell'assegnazione di un nodo:** dall'elenco Nodi selezionati, individuare il nodo di cui si desidera annullare l'assegnazione dal criterio.

     Fare clic sulla freccia sinistra singola.

     Il nodo verrà spostato dall'elenco Nodi selezionati all'elenco Nodi disponibili.

   - **Annullamento dell'assegnazione di nodi:** dall'elenco Nodi selezionati, fare clic sulla freccia sinistra doppia.

     Tutti i nodi vengono spostati dall'elenco Nodi selezionati all'elenco Nodi disponibili.

   Fare clic su OK.

L'assegnazione dei nodi dal criterio viene eseguita o annullata.

Distribuzione dei criteri

Dopo la creazione di un criterio, è possibile assegnare i nodi a un criterio (a pagina 53) e quindi distribuire il criterio.

Il comportamento descritto di seguito è valido per il processo di distribuzione del criterio:

- Il processo di distribuzione del criterio non può essere completato se si verificano le condizioni riportate di seguito.
  - Il ruolo Windows Server 2008 Hyper-V è installato sul server di origine di CA ARCserve D2D (nodo).
  - Il nodo CA ARCserve D2D è stato importato da CA ARCserve Central Host-Based VM Backup. Il ruolo Windows Hyper-V è abilitato sul sistema proxy di backup dei computer virtuali basato sull'host e il sistema proxy di backup è stato specificato come destinazione di standby virtuale.
- CA ARCserve Central Virtual Standby non è in grado di attivare automaticamente i computer virtuali aggiunti dai server CA ARCserve Central Host-Based VM Backup. Di conseguenza, quando si esegue la distribuzione dei criteri con metodo di recupero impostato su Avvia il computer virtuale automaticamente sui nodi protetti da backup dei computer virtuali basato sull'host, Virtual Standby modifica il metodo di recupero su Avvia il computer virtuale manualmente.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby, quindi aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Criteri per visualizzare la schermata corrispondente.

2. Dall'elenco Criteri, fare clic sul criterio che si desidera distribuire.

   Le informazioni dettagliate relative al criterio specificate verranno visualizzate nelle schede Dettagli criterio e Assegnazione criterio.

3. Fare clic sulla scheda Dettagli criterio per visualizzare informazioni dettagliate relative al criterio.

   (Facoltativo) Fare clic su Modifica della barra degli strumenti per modificare le impostazioni correnti per il criterio.

   Nota: per ulteriori informazioni, consultare la sezione Modifica dei criteri.

4. Fare clic sulla scheda Assegnazione criterio.

   Verranno visualizzate le informazioni dettagliate relative ai nodi assegnati al criterio.

   (Facoltativo) Fare clic su Assegna e Annulla assegnazione per assegnare o annullare l'assegnazione dei nodi al criterio.

   Nota: per ulteriori informazioni, consultare la sezione Assegnazione di nodi ai criteri (a pagina 53) o Annullamento dell'assegnazione dei nodi dai criteri.

5. Fare clic su Distribuisci ora della barra degli strumenti.

   Verrà visualizzato il messaggio di conferma Distribuisci ora.

6. Fare clic su OK (Salva/Applica).

Il criterio viene distribuito.

Nota: è inoltre possibile visualizzare lo stato di distribuzione del criterio per un nodo specifico nella schermata Nodo della colonna Criterio.

Capitolo 4: Introduzione a CA ARCserve Central Virtual Standby

Le seguenti sezioni descrivono le modalità di configurazione di CA ARCserve Central Virtual Standby per la protezione dei nodi CA ARCserve D2D.

Nota: prima di completare le configurazioni descritte in questa sezione, assicurarsi che siano state eseguite tutte le attività preliminari all'installazione (a pagina 15).

Questa sezione contiene i seguenti argomenti:

Accesso a CA ARCserve Central Virtual Standby.

È possibile accedere a CA ARCserve Central Virtual Standby direttamente dal computer su cui è installata l'applicazione o da un computer remoto mediante un browser supportato. Per un elenco completo dei browser supportati, consultare le *Note di rilascio di CA ARCserve Central Virtual Standby*.

Per accedere a CA ARCserve Central Virtual Standby

1. Selezionare una delle seguenti opzioni:

   - Se si esegue l'accesso al server di installazione di CA ARCserve Central Virtual Standby, avviare l'applicazione dai file di programma.

     Si aprirà una finestra del browser contenente la schermata di accesso a CA ARCserve Central Virtual Standby.

     Completare i seguenti campi della schermata:

     - Nome utente
     - Password

     Fare clic su Accedi.

   - Se l'accesso al server su cui è installato CA ARCserve Central Virtual Standby non è stato eseguito, aprire una finestra del browser e immettere il seguente indirizzo URL nella barra degli indirizzi:

     ```
     http://<CA ARCserve Central Application Server Name>:<Port
     Number>/virtualstandby/
     ```

     Nota: durante l'installazione di CA ARCserve Central Virtual Standby, è possibile specificare il nome host o l'indirizzo IP del server. Il numero predefinito della porta è 8015.

     Premere Invio.

     Si aprirà una finestra del browser contenente la schermata di accesso a CA ARCserve Central Virtual Standby.

     Completare i seguenti campi della schermata:

     - Nome utente
     - Password

     Fare clic su Accedi.

   Verrà visualizzata la pagina principale di CA ARCserve Central Virtual Standby.

Specificare il sistema server ESX o vCenter per i nodi basati su VMware.

Nota: la procedura che segue è applicabile solo ai nodi di origine dei computer virtuali basati su VMware.

In varie implementazioni basate su VMware, Virtual Standby potrebbe non essere in grado di rilevare i nodi di origine configurati come computer virtuali che risiedono su sistemi ESX Server e vCenter Server. Questo comportamento impedisce a Virtual Standby di applicare la licenza corretta ai nodi, di distribuire i criteri ai nodi e di eseguire i processi di conversione.

La procedura seguente consente di specificare il nome host o l'indirizzo IP del sistema server ESX o vCenter su cui risiedono i nodi. Al termine della procedura, Virtual Standby potrà rilevare, applicare le licenze, distribuire i criteri ed eseguire i processi di conversione per i nodi che si desidera proteggere. Se sono presenti più computer virtuali che risiedono su un sistema server ESX o vCenter e che operano come singolo nodo di origine, la procedura consente di utilizzare una licenza per tutti i nodi, riducendo i costi complessivi per la protezione dei nodi di origine.

Per specificare il sistema server ESX o vCenter per i nodi basati su VMware

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente il nodo da aggiornare.

   I nodi associati con il gruppo verranno visualizzati nell'elenco dei nodi.

3. Fare clic sul nodo da aggiornare, quindi su Specifica server ESX dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Specifica server ESX.

   Nota: se l'applicazione rileva che gli strumenti VMware non sono installati sul computer virtuale gestito dal sistema server ESX o vCenter, se il computer virtuale risiede su un sistema Hyper-V oppure il nodo rilevato non è un computer virtuale, viene visualizzato un messaggio di errore.

4. Completare i seguenti campi della finestra di dialogo Specifica server ESX:
   - Host ESX/vCenter

     Nota: specificare il nome host o l'indirizzo IP del sistema ESX Server o vCenter Server.
   - Nome utente
   - Password
   - Porta

     Nota: la porta di comunicazione predefinita è la 443. Se il nodo comunica con il sistema server ESX o vCenter utilizzando un numero di porta differente, specificare il numero di porta utilizzato.
   - Protocollo

     Nota: il protocollo di comunicazione predefinito è HTTPS. Se il nodo comunica con il sistema server ESX o vCenter mediante HTTP, fare clic su HTTP.

   Fare clic su OK.

Il sistema server ESX o vCenter viene assegnato al nodo.

Capitolo 5: Mediante CA ARCserve Central Virtual Standby

Questa sezione contiene i seguenti argomenti:

Accesso ai nodi CA ARCserve D2D

Dalla pagina principale di Virtual Standby è possibile accedere ai nodi CA ARCserve D2D.

Per accedere ai nodi CA ARCserve D2D

1. Aprire l'applicazione e fare clic su Nodi sulla barra di spostamento.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

L'utente è connesso al nodo CA ARCserve D2D.

Nota: è possibile che durante il primo accesso al nodo CA ARCserve D2D venga visualizzata una pagina HTML contenente un messaggio di avviso. Questo comportamento si verifica con l'utilizzo di Internet Explorer. Per risolvere il problema, chiudere Internet Explorer e ripetere il passaggio 3. Sarà quindi possibile accedere al nodo CA ARCserve D2D correttamente.

Accesso ai server di monitoraggio

Virtual Standby consente di accedere direttamente al server di monitoraggio dei nodi di origine di CA ARCserve D2D. Dal server di monitoraggio è possibile eseguire attività di manutenzione e visualizzare le informazioni sullo stato del server di origine monitorati dal server di monitoraggio. Le seguenti icone consentono di distinguere i nodi CA ARCserve D2D dai server di monitoraggio:

Icona Server di monitoraggio:



Icona del nodo CA ARCserve D2D:



Per accedere ai server di monitoraggio

1. Accedere al server di Virtual Standby, quindi aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Nodi.

   Verrà visualizzata la schermata Nodi.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Eseguire una delle seguenti operazioni:

   - Se si dispone dell'indirizzo IP o del nome host del server di monitoraggio, identificare e selezionare il server di monitoraggio a cui si desidera eseguire l'accesso, quindi fare clic su Accesso a D2D dal menu di scelta rapida.

   - Se non si conosce l'indirizzo IP o il nome host del server di monitoraggio, individuare a e selezionare il nodo di CA ARCserve D2D corrispondente al server di monitoraggio a cui si desidera accedere, quindi fare clic su Accedere al server di monitoraggio nel menu di scelta rapida.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

L'utente è connesso al server di monitoraggio.

Attività di manutenzione dei nodi

Virtual Standby consente l'utilizzo di diversi metodi per l'aggiunta di nodi:

- Aggiunta di nodi per indirizzo IP o nome nodo (a pagina 33).
- Aggiunta di nodi da un file (a pagina 34).

  Nota: questo metodo consente di importare più nodi da un elenco di nodi in un file con valori delimitati da virgole.
- Aggiunta di nodi dai server CA ARCserve Central Host-Based VM Backup (a pagina 36).

  Nota: questo metodo consente di importare i nodi del computer virtuale protetti dall'applicazione CA ARCserve Central Host-Based VM Backup.
- Importazione dei nodi da CA ARCserve Replication and High Availability (a pagina 39).

Inoltre, è possibile eseguire le seguenti attività di gestione nodo:

- Aggiornamento dei nodi (a pagina 63).
- Aggiunta della sezione Impostazione delle password di backup per uno o più nodi di CA ARCserve D2D (a pagina 66).
- Eliminazione dei nodi (a pagina 67).
- Rilascio di licenze dai nodi (a pagina 68).
- Interruzione del monitoraggio di nodi dal server di monitoraggio (a pagina 70).
- Aggiornamento di nodi e criteri dopo la modifica del nome host del server CA ARCserve Central Applications (a pagina 70).

Aggiornamento dei nodi

Virtual Standby consente di aggiornare le informazioni relative ai nodi aggiunti precedentemente.

Nota: non è possibile aggiornare i nodi che sono stati importati da un server CA ARCserve Central Host-Based VM Backup.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente i nodi che si desidera aggiornare.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Fare clic sul nodo da aggiornare, quindi fare clic con il tasto destro del mouse su Aggiorna nodo dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiorna nodo.

   Nota: per aggiornare tutti i nodi del gruppo di nodi, fare clic con il tasto destro del mouse sul nome del gruppo di nodi e selezionare Aggiorna nodo dal menu di scelta rapida.

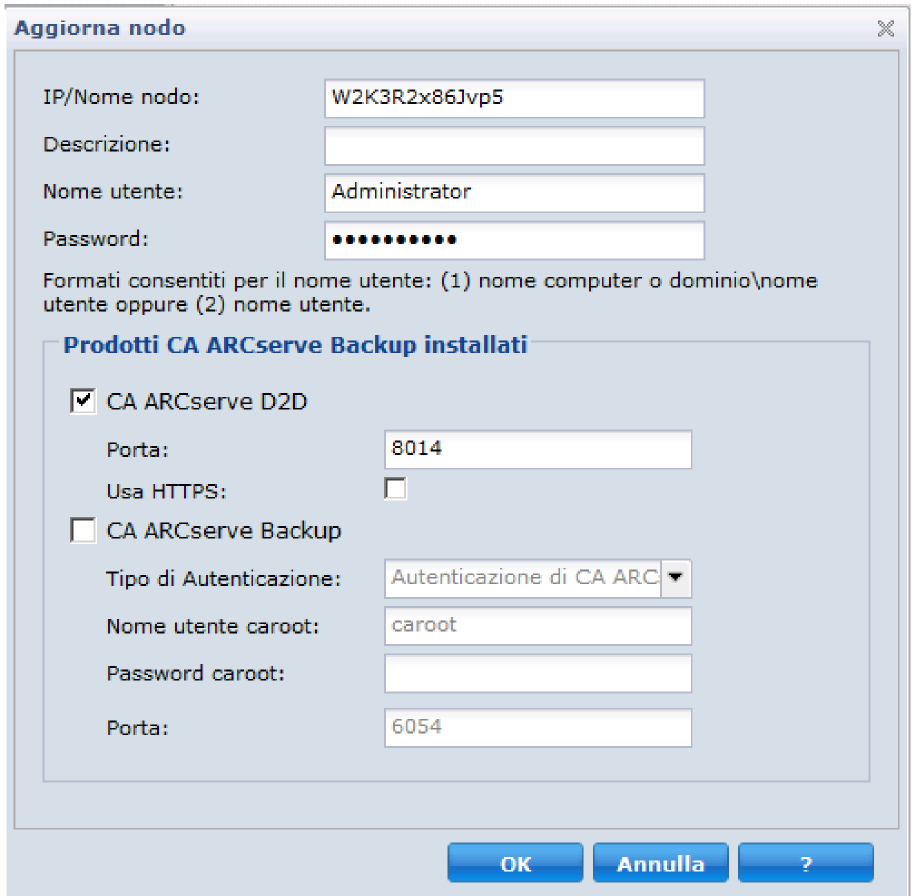
4. Aggiornare i dettagli del nodo.

   Nota: per aggiornare nodi multipli dell'Elenco nodi, selezionare i nodi desiderati, fare clic con il tasto destro del mouse su qualsiasi nodo, quindi selezionare Aggiorna nodo dal menu di scelta rapida. Il nome utente e la password coincidono per i nodi selezionati. L'opzione Specifica nuove credenziali e la casella di controllo Acquisisci controllo del nodo sono selezionate per impostazione predefinita. È possibile specificare un nuovo nome utente e una nuova password per i nodi selezionati ed imporre al server la gestione dei nodi specificati. Inoltre, è possibile selezionare l'opzione Usa le credenziali esistenti per applicare il nome utente e la password correnti. I campi vengono disattivati.

5. Fare clic su OK.

   La finestra di dialogo Aggiorna nodo verrà chiusa e i nodi verranno aggiornati.

   Nota: se sono state apportate modifiche ai nodi di CA ARCserve D2D, verrà visualizzata la finestra di dialogo Aggiorna nodo, in cui è possibile specificare ulteriori dettagli.



6. (Facoltativo) Se le informazioni aggiornate non compaiono nell'elenco dei nodi, fare clic su Aggiorna nella barra degli strumenti.

Il nodo verrà aggiornato.

Impostazione delle password di backup per uno o più nodi di CA ARCserve D2D

Durante l'inoltro dei backup di D2D, la password di backup viene archiviata sul nodo D2D protetto. CA ARCserve Replication and High Availability replica i punti di ripristino D2D sul sito MSP (Managed Service Provider). Il convertitore sul sito MSP converte i dati replicati in dati di computer virtuale e li archivia sul sito MSP. Tuttavia, il convertitore non è in grado di convertire le snapshot dei punti di ripristino replicati in quanto le password di backup risiedono sul nodo D2D.

Per consentire al convertitore di convertire le snapshot dei punti di ripristino replicati, Virtual Standby consente di specificare le password di backup per i dati di D2D che possono essere utilizzati dal convertitore per la conversione dei dati.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

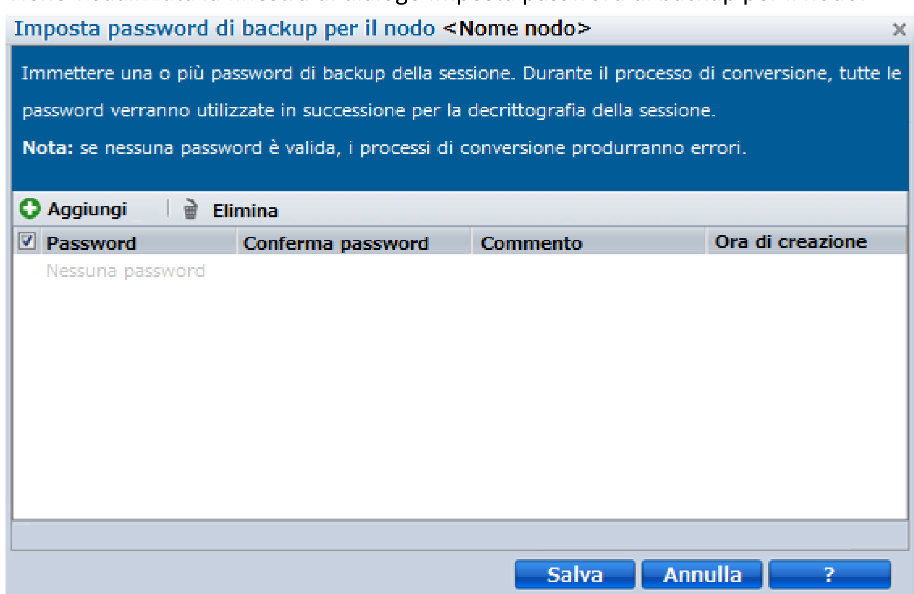
   Verrà visualizzata la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo Tutti i nodi oppure sul nome del gruppo contenente i nodi per cui si desidera impostare le password di backup.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Fare clic sui nodi per cui si desidera impostare le password di backup, quindi fare clic con il tasto destro del mouse e selezionare Imposta password di backup dal menu di scelta rapida.

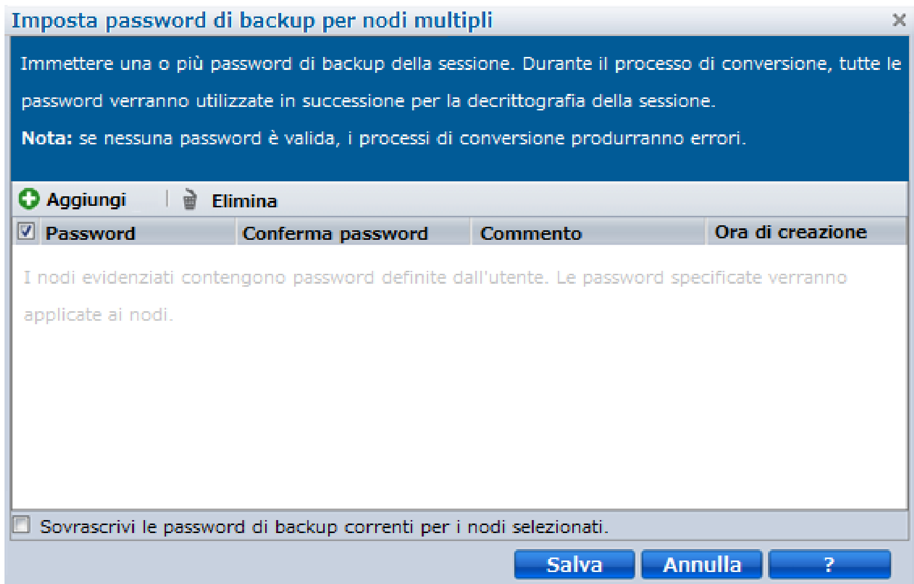
   Viene visualizzata la finestra di dialogo Imposta password di backup per il nodo.



La finestra di dialogo Imposta password di backup per il nodo consente di effettuare le azioni seguenti per uno o più nodi:

- **Aggiungi**: fare clic su Aggiungi per aggiungere uno o più password di backup ai nodi selezionati.
- **Elimina**: fare clic su Elimina per eliminare una o più password di backup dai nodi selezionati.

Nota: in caso di nodi multipli, è possibile sovrascrivere le password di backup correnti per i nodi multipli selezionando la casella di controllo Sovrascrivi le password di backup correnti per i nodi selezionati.



4. Fare clic su Salva.

   La finestra di dialogo viene chiusa e le password di backup vengono impostate per i nodi remoti selezionati.

Eliminazione dei nodi

Virtual Standby consente di eliminare nodi dall'ambiente.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Fare clic su Nodo sulla barra di navigazione per aprire la schermata Nodo.

2. Dalla barra Gruppi, fare clic sul gruppo di Tutti i nodi oppure sul nome del gruppo contenente il nodo da eliminare.

   I nodi associati al gruppo verranno visualizzati nell'elenco dei nodi.

3. Selezionare i nodi che si desidera eliminare, quindi fare clic su Elimina sulla barra degli strumenti.

   Verrà visualizzato un messaggio di conferma.

4. Eseguire una delle seguenti operazioni:

   - Fare clic su Sì per eliminare il nodo.
   - Fare clic su No se non si desidera eliminare il nodo.

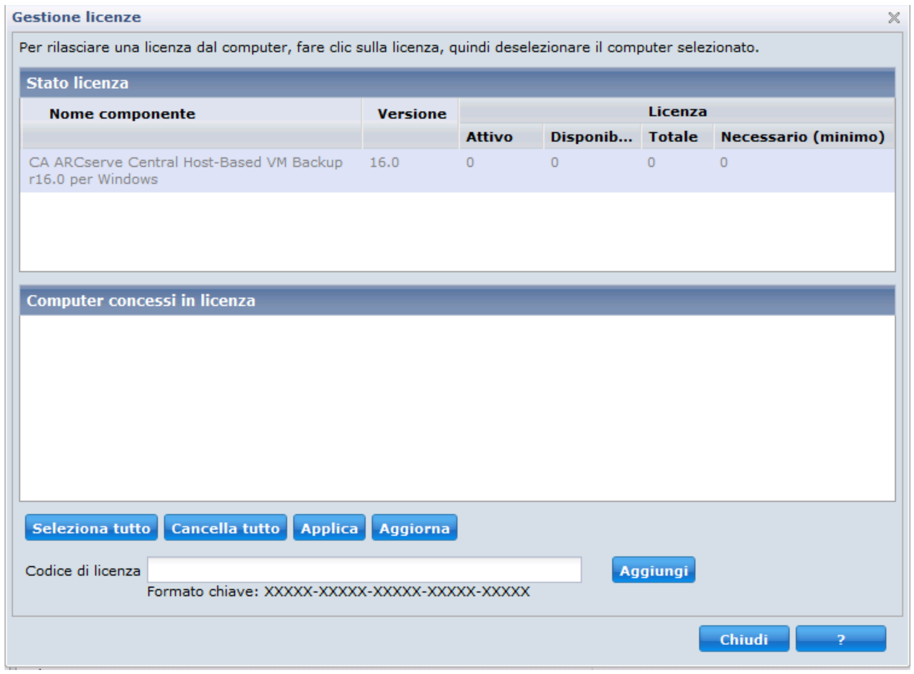
Rilascio di licenze dai nodi

Le licenze di CA ARCserve Central Virtual Standby utilizzano un metodo basato su conteggio. Le licenze basate su conteggio consentono di concedere una singola licenza globale al nodo con un numero predeterminato di diritti di licenza inclusi nel pool di licenze globale. A ciascun nodo che utilizza la licenza viene concessa una licenza attiva dal pool, in base all'ordine di richiesta, fino al raggiungimento del numero totale di diritti di licenza disponibili. Se sono stati utilizzati tutti i diritti di licenza attivi e si desidera aggiungere una licenza a un altro nodo, è necessario innanzi tutto rilasciare i diritti di licenza da uno o più nodi per aumentare il numero di licenze disponibili.

Come rilasciare licenze dai nodi

1. Accedere all'applicazione.
2. Nella schermata iniziale fare clic su ? e quindi su Gestisci licenze per visualizzare la finestra di dialogo Gestisci licenze.

   Viene visualizzata la finestra di dialogo Gestisci licenze contenente un elenco delle licenze applicate ai computer fisici, ai computer virtuali basati su VMware e ai computer virtuali basati su Hyper-V, come illustrato nella seguente finestra di dialogo:



3. Nella sezione relativa allo stato delle licenze, selezionare la licenza che si desidera rilasciare dai nodi.

   Nella sezione Computer concessi in licenza della finestra di dialogo Gestisci licenze vengono visualizzati i nodi che utilizzano la licenza.

4. Fare clic sulla casella di controllo accanto al nodo di cui si desidera rilasciare la licenza.

   Nota: fare clic su Cancella tutto per deselezionare le caselle di controllo accanto a tutti i nodi visualizzati nella sezione Computer concessi in licenza della finestra di dialogo Gestisci licenze.

5. Fare clic su Applica.

   La licenza viene rilasciata dal nodo specificato.

6. (Facoltativo) Fare clic su Aggiorna per aggiornare l'elenco dei nodi che utilizzano la licenza specificata.

Interruzione del monitoraggio di nodi dal server di monitoraggio

CA ARCserve Central Virtual Standby consente di interrompere il monitoraggio dei nodi dalla scheda Virtual Standby del server di monitoraggio.

Importante: Quando si interrompe il monitoraggio dei nodi, i computer di standby virtuale potrebbero non contenere le snapshot più recenti del punto di ripristino, necessarie per l'attivazione dei computer virtuali. Inoltre, i computer virtuali corrispondenti ai nodi di cui è stato interrotto il monitoraggio (manualmente) potranno essere attivati solo dal sistema hypervisor.

Per interrompere il monitoraggio dei nodi dal server di monitoraggio

1. Accedere al server di monitoraggio.

   Nota: Per ulteriori informazioni, consultare la sezione Accesso ai server di monitoraggio (a pagina 62).

2. Una volta aperto il server di monitoraggio, fare clic sulla scheda Virtual Standby.

   Verrà visualizzata la schermata Virtual Standby.

3. Dalla struttura Origini, espandere Tutto, Origine in esecuzione, Richiede azione, oppure Computer virtuale in esecuzione per individuare il nodo di origine di cui arrestare il monitoraggio.

4. Fare clic con il tasto destro del mouse sul nodo di cui si desidera arrestare il monitoraggio, quindi fare clic su Arresta monitoraggio dal menu di scelta rapida.

   Verrà visualizzato un messaggio di avviso.

5. Per confermare l'arresto del monitoraggio del nodo specificato, fare clic su Sì.

Il nodo viene rimosso dalla struttura Origini e il server di monitoraggio interromper il monitoraggio del nodo.

Aggiornamento di nodi e criteri dopo la modifica del nome host del server CA ARCserve Central Applications

Una volta modificato il nome host del server CA ARCserve Central Virtual Standby, aggiornare i nodi e i criteri applicati ai nodi. È necessario eseguire tali attività per mantenere la relazione tra il server CA ARCserve Central Virtual Standby e i nodi protetti da tale server. La tabella seguente descrive gli scenari possibili e le azioni applicabili a ciascuno scenario.

Scenario	Misura correttiva
Il nodo è stato aggiunto dopo la modifica del nome host del server CA ARCserve Central Virtual Standby.	Non è richiesto alcun intervento.

Scenario	Misura correttiva
Il nodo è stato aggiunto prima della modifica del nome host del server CA ARCserve Central Virtual Standby, senza applicare criteri.	Aggiornare il nodo. Per ulteriori informazioni, consultare la sezione Aggiornamento dei nodi (a pagina 63).
Il nodo è stato aggiunto prima che il nome host del server CA ARCserve Central Virtual Standby fosse modificato e un criterio fosse applicato al nodo.	Applicare nuovamente il criterio. Per ulteriori informazioni, consultare la sezione Distribuzione dei criteri (a pagina 55).

Attività di gestione del gruppo di nodi

Virtual Standby consente la gestione dei gruppi di nodi di CA ARCserve D2D protetti.

In questa sezione verranno presentati i seguenti argomenti:

Aggiunta di gruppi di nodi

I gruppi di nodi consentono di gestire un insieme di computer origine CA ARCserve D2D in base a caratteristiche comuni. Ad esempio, è possibile definire gruppi di nodi classificati in base al dipartimento che supportano: Contabilità, Marketing, Legale, Risorse umane, ecc.

L'applicazione contiene i seguenti gruppi di nodi:

- **Gruppi predefiniti:**
  - **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
  - **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
  - **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
  - **SQL Server** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.
  - **Exchange** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft Exchange Server.

  Nota: i gruppi di nodi predefiniti non possono essere modificati o eliminati.
- **Gruppi personalizzati** - Contiene i gruppi di nodi personalizzati.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.

2. Fare clic su Aggiungi nella barra degli strumenti Gruppo nodi.

   Si aprirà la finestra di dialogo Aggiungi gruppo e verranno visualizzati i nodi nell'elenco Nodi disponibili.

3. Specificare un Nome gruppo per il gruppo di nodi.

4. Completare i seguenti campi della finestra di dialogo Aggiungi gruppo:

   - **Gruppo:**selezionare il nome del gruppo contenente i nodi da assegnare.
   - **Filtro Nome nodo:** consente di filtrare i nodi disponibili in base a un criterio comune.

     Nota: il campo Nome nodo supporta l'uso di caratteri jolly.

     Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare i risultati del filtro, fare clic su sul simbolo X del campo Filtro.

5. Per aggiungere nodi al gruppo di nodi, selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra singola.

   I nodi verranno spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati e assegnati al gruppo di nodi.

   Nota: per selezionare e spostare tutti i nodi dal gruppo corrente, fare clic sulla freccia destra doppia.

6. Se si desidera spostare tutti i nodi dall'elenco Nodi selezionati all'elenco Nodi disponibili fare clic sulla freccia sinistra singola.

   Nota: per selezionare e spostare tutti i nodi dal gruppo corrente, fare clic sulla freccia sinistra doppia.

7. Fare clic su OK.

Il gruppo di nodi verrà aggiunto.

Modifica di gruppi di nodi

L'applicazione consente di modificare i gruppi di nodi creati. È possibile aggiungere o rimuovere i nodi dai gruppi di nodi e modificare il nome dei gruppi.

Nota - I seguenti gruppi di nodi non possono essere modificati:

- **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
- **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
- **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
- **SQL Server** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.
- **Exchange** - Contiene tutti i nodi associati con l'applicazione e che dispongono di Microsoft SQL Server.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Fare clic sul gruppo di nodi da modificare, quindi selezionare Modifica nella barra degli strumenti Gruppo nodi.

   Verrà visualizzata la finestra di dialogo Modifica gruppo.

3. Per modificare il nome del gruppo, specificare un nuovo nome nel campo Nome gruppo.

4. Per aggiungere nodi al gruppo nodi, selezionare i nodi che si desidera aggiungere e fare clic sulla freccia destra.

   I nodi verranno spostati dall'elenco Nodi disponibili all'elenco Nodi selezionati e assegnati al gruppo di nodi.

   Nota: per spostare tutti i nodi dall'elenco Nodi disponibili all'elenco Nodi selezionati fare clic sulla freccia destra doppia.

5. Per rimuovere nodi dal gruppo di nodi, fare clic sulla freccia sinistra oppure sulla freccia sinistra doppia per rimuovere rispettivamente uno o tutti i nodi.

6. (Facoltativo) Per filtrare i nodi disponibili in base a criteri comuni, specificare un valore nel Filtro Nome nodo.

   Nota: il campo Filtro supporta l'uso di caratteri jolly.

   Ad esempio, Acc* consente di filtrare tutti i nodi il cui nome inizia per Acc. Per cancellare tutti i risultati del filtro, fare clic sul simbolo X del campo Filtro.

7. Fare clic su OK.

Il gruppo di nodi verrà modificato.

Eliminazione di gruppi di nodi

L'applicazione consente di eliminare i gruppi di nodi creati.

Non è possibile eliminare i seguenti gruppi di nodi:

- **Tutti i nodi** - Contiene tutti i nodi associati con l'applicazione.
- **Nodi senza un gruppo** - Contiene tutti i nodi associati all'applicazione non assegnati a un gruppo di nodi.
- **Nodi senza un criterio** - Contiene tutti i nodi associati all'applicazione che non dispongono di un criterio assegnato.
- **SQL Server** - Contiene tutti i nodi associati con l'applicazione i cui nodi dispongono di Microsoft SQL Server.
- **Exchange** - Contiene tutti i nodi associati con l'applicazione i cui nodi dispongono di Microsoft Exchange Server.

Nota: il processo di eliminazione dei gruppi di nodi non comporta l'eliminazione dei singoli nodi dall'applicazione.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo per aprire la schermata Nodo.

2. Fare clic sul gruppo di nodi da eliminare, quindi su Elimina nella barra degli strumenti Gruppo nodi.

   Verrà visualizzata una finestra di dialogo di conferma.

3. Se si è sicuri di voler eliminare il gruppo dei nodi, fare clic su Sì.

   Nota: fare clic su No se non si desidera cancellare il gruppo di nodi.

Il gruppo dei nodi viene eliminato.

Filtraggio di gruppi di nodi

Virtual Standby consente l'utilizzo di filtri per visualizzare i nodi CA ARCserve D2D di un gruppo su cui è installata una determinata applicazione. Virtual Standby consente di filtrare i nodi su cui sono installate le seguenti applicazioni:

- CA ARCserve Backup
- CA ARCserve D2D
- Microsoft SQL Server
- Microsoft Exchange Server

Per filtrare i gruppi di nodi

1. Accedere al server di Virtual Standby, quindi aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Nodo.

   Verrà visualizzata la schermata Nodo.

2. Nell'elenco Gruppi selezionare il gruppo che si desidera filtrare.

   Nota: è possibile filtrare tutti i gruppi predefiniti (Tutti i nodi, Non assegnato, SQL Server e Exchange) e i gruppi con nome personalizzato.

   Dalla barra degli strumenti Filtro, selezionare la casella di controllo corrispondente all'applicazione che si desidera filtrare.

Il gruppo dei nodi viene filtrato.

Attività di gestione criteri di Virtual Standby

Virtual Standby consente di gestire i criteri di conversione utilizzati per proteggere i nodi CA ARCserve D2D.

Modifica o copia di criteri

Virtual Standby consente di modificare o copiare i criteri dopo averli creati.

Per modificare i criteri

1. Accedere al server Virtual Standby, quindi aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Criteri.

   Verrà visualizzata la finestra dei criteri.

2. Dalla schermata Criteri, fare clic sulla casella di controllo corrispondente al criterio, quindi eseguire una delle seguenti operazioni:

   - Fare clic su Modifica della barra degli strumenti per modificare il criterio selezionato.
   - Fare clic su Copia della barra degli strumenti per copiare e creare un nuovo criterio dal criterio selezionato.

     Nota: la finestra di dialogo Copia criterio viene visualizzata quando viene eseguita la copia di un criterio. Specificare un nuovo nome per il criterio e fare clic su OK.

   Verrà visualizzata la finestra di dialogo Modifica criterio.

Se si desidera modificare il nome del criterio, specificare un nome nel campo Nome criterio.

3. Se si desidera modificare il nome del criterio, specificare un nome nel campo Nome criterio.

4. Applicare le modifiche alla scheda Virtual Standby e alla scheda Preferenze, in base al tipo di criterio selezionato.

   - Criterio locale di Virtual Standby (a pagina 40)
   - Criterio remoto di Virtual Standby (a pagina 47)

Il criterio viene modificato.

Eliminazione dei criteri

Virtual Standby consente di eliminare i criteri creati precedentemente.

Nota: Virtual Standby non consente l'eliminazione di criteri assegnati a nodi. Per eliminare i criteri a cui sono assegnati nodi, è necessario annullare l'assegnazione dei nodi dal criterio, quindi eliminare il criterio. Per informazioni sulla modalità di annullamento dell'assegnazione dei nodi da un criterio, consultare la sezione Annullamento dell'assegnazione dei nodi dai criteri.

Per eliminare i criteri

1. Accedere al server di Virtual Standby, quindi aprire Virtual Standby.

   Dalla barra di navigazione della pagina principale, fare clic su Criteri VCM.

   Verrà visualizzata la finestra dei criteri.

2. Dall'elenco Criteri, fare clic sul criterio che si desidera eliminare.

3. Fare clic su Elimina della barra degli strumenti Criteri.

   Verrà visualizzato un messaggio di conferma di eliminazione.

4. Fare clic su Sì per eliminare il criterio.

   Nota: se un criterio viene eliminato per sbaglio, sarà necessario creare nuovamente il criterio. Se non si desidera eliminare il criterio, fare clic su No.

Il criterio viene eliminato.

Attività di configurazione delle applicazioni

Virtual Standby consente di specificare le impostazioni degli avvisi di posta elettronica e le modalità di aggiornamento dell'installazione di Virtual Standby.

In questa sezione verranno presentati i seguenti argomenti:

Configurazione delle impostazioni di posta elettronica

Le impostazioni di posta elettronica possono essere configurate per l'invio automatico degli avvisi nel caso in cui si verifichino le condizioni specificate.

Procedere come descritto di seguito:

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, fare clic su Configurazione per aprire la schermata corrispondente.

2. Nel riquadro Configurazione, fare clic su Configurazione di posta elettronica per visualizzare le opzioni di configurazione corrispondenti.

3. Completare i seguenti campi:

   - **Servizio** - Specificare il tipo di servizio di posta elettronica dall'elenco a discesa. (Google Mail, Yahoo Mail, Live Mail o Altri).
   - **Server di posta** - Specificare il nome host del server SMTP utilizzato da CA ARCserve Central Applications per l'invio di messaggi di posta elettronica.
   - **Richiede l'autenticazione** - Selezionare questa opzione se il server di posta specificato richiede l'autenticazione. Il Nome account e la Password sono obbligatori.
   - **Oggetto** - Specificare un oggetto di posta elettronica predefinito.
   - **Da** - Specificare l'indirizzo di posta elettronica di invio del messaggio.
   - **Destinatari** - Specificare uno o più indirizzi di posta elettronica, separati da un punto e virgola (;), per l'invio di messaggi di posta elettronica.
   - **Usa SSL** - Selezionare questa opzione se il server di posta specificato richiede la connessione protetta (SSL).
   - **Invia STARTTLS** - Selezionare questa opzione se il server di posta specificato richiede il comando STARTTLS.
   - **Usa formato HTML** - Consente di inviare messaggi di posta elettronica in formato HTML. (selezionato per impostazione predefinita)
   - **Abilita impostazioni proxy** - Selezionare questa opzione se è presente un server proxy, quindi specificare le impostazioni corrispondenti.

4. Fare clic su Messaggio di posta elettronica di verifica per verificare che le impostazioni di configurazione siano corrette.

5. Fare clic su Salva.

   Nota: è possibile fare clic su Reimposta per tornare ai valori salvati in precedenza.

La configurazione del server di posta verrà applicata.

Configurazione degli aggiornamenti automatici

CA ARCserve Central Virtual Standby consente di pianificare l'esecuzione degli aggiornamenti di prodotto e la frequenza di aggiornamento dell'installazione di Virtual Standby.

Per configurare gli aggiornamenti automatici

1. Accedere all'applicazione.
2. Fare clic su Configurazione sulla barra di navigazione per aprire la schermata Configurazione.
3. Dal pannello di configurazione, fare clic su Configurazione aggiornamento.

   Verranno visualizzate le opzioni di configurazione degli aggiornamenti.
4. Selezionare un server di download.
   - **CA Server** - Fare clic su Impostazioni proxy per visualizzare le opzioni seguenti:
     - **Utilizza le impostazioni proxy del browser** - Consente di utilizzare le credenziali immesse per il proxy del browser.

       Nota: l'opzione Utilizza le impostazioni proxy del browser influisce sul funzionamento di Internet Explorer e Chrome.
     - **Configura impostazioni proxy** - Specificare l'indirizzo IP o il nome host del server proxy e il numero di porta. Se il server specificato richiede l'autenticazione, selezionare l'opzione Il server proxy richiede l'autenticazione e immettere le credenziali.

       Fare clic su OK per tornare alla configurazione aggiornamenti.
   - **Server di gestione temporanea** - Se si sceglie questa opzione, fare clic su Aggiungi server per aggiungere un server di gestione temporanea all'elenco. Immettere il nome host e il numero di porta del server, quindi fare clic su OK.

     Se si specificano più server di gestione temporanea, l'applicazione tenterà di utilizzare il primo server contenuto nell'elenco. Se la connection viene eseguita correttamente, i server restanti non verranno utilizzati per la gestione temporanea.
5. (Facoltativo) Per verificare la connessione del server, fare clic su Verifica connessione e attendere il completamento della verifica.
6. (Facoltativo) Fare clic Verifica aggiornamenti automaticamente e specificare il giorno e l'ora desiderati. La pianificazione può essere effettuata su base giornaliera o settimanale.

Fare clic su Salva per applicare la configurazione di aggiornamento.

Configura impostazioni proxy

CA ARCserve Central Applications consente di specificare un server proxy per la comunicazione con il supporto tecnico di CA per verificare la disponibilità di aggiornamenti e scaricarli. Per attivare questa funzionalità, specificare il server proxy che si desidera impostare per la comunicazione del server CA ARCserve Central Applications.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Configurazione sulla barra di spostamento.

   Verranno visualizzate le opzioni di configurazione.

2. Fare clic su Configurazione aggiornamento.

   Verrà visualizzata la finestra di dialogo Configurazione aggiornamento.

3. Fare clic su Impostazioni proxy.

   Verrà visualizzata la finestra di dialogo Impostazioni proxy.

4. Selezionare una delle seguenti opzioni:

   - **Utilizza le impostazioni proxy del browser** - Consente all'applicazione di rilevare e utilizzare le stesse impostazioni proxy applicate al browser per connettersi al server di CA Technologies per aggiornare le informazioni.

     Nota: questo comportamento è valido solo per i browser Internet Explorer e Chrome.

   - **Configura impostazioni proxy** - Consente di definire un server alternativo che l'applicazione utilizzerà per comunicare con il Supporto tecnico di CA per verificare la disponibilità di aggiornamenti. Il server alternativo (proxy) garantisce protezione e migliora le prestazioni e il controllo amministrativo.

     Completare i seguenti campi:

     - **Server proxy** - Specificare il nome host o l'indirizzo IP del server proxy.
     - **Porta** - Specificare il numero di porta che il server proxy utilizzerà per comunicare con il sito Web del Supporto tecnico di CA.
     - **(Facoltativo) Il server proxy richiede l'autenticazione -** Se le credenziali di accesso per il server proxy non sono uguali a quelle per il server CA ARCserve Central Applications, selezionare la casella di controllo Il server proxy richiede l'autenticazione e specificare il nome utente e la password per l'accesso al server proxy.

       Nota: per specificare il nome utente utilizzare il formato <nome dominio>/<nome utente>.

   Fare clic su OK.

Le impostazioni proxy sono configurate.

Configurazione delle preferenze di Social network

CA ARCserve Central Applications consente di gestire gli strumenti di Social network che possono agevolare la gestione delle singole applicazioni. È possibile generare newsfeed, specificare collegamenti a siti Web di social network popolari e selezionare siti Web video.

Per configurare le preferenze di Social network

1. Accedere all'applicazione.

   Dalla barra di navigazione della pagina principale, selezionare Configurazione.

   Verrà visualizzata la finestra di dialogo Configurazione.

2. Dal pannello Configurazione, fare clic su Configurazione delle preferenze.

   Vengono visualizzate le opzioni relative alle preferenze.



3. Specificare le opzioni desiderate:

   - **Newsfeed** - L'applicazione visualizza i feed RSS relativi alle notizie più recenti di CA ARCserve Central Applications e CA ARCserve D2D e le informazioni sui prodotti dal Centro di consultazione esperti. I feed verranno visualizzati nella pagina principale.
   - **Social network** - L'applicazione visualizza nella pagina principale le icone di accesso a Twitter e Facebook per i siti Web di social network relativi a CA ARCserve Central Applications e CA ARCserve D2D.
   - **Video** - Consente di selezionare il tipo di video per la visualizzazione dei prodotti CA ARCserve Central Applications e CA ARCserve D2D (Impostazione predefinita: Video di YouTube).

   Fare clic su Salva.

   Le opzioni di Social network verranno applicate

4. Dalla barra di navigazione fare clic su pagina iniziale.

   Verrà visualizzata la pagina iniziale.

5. Aggiornare il browser.

   Le opzioni di Social network verranno applicate.

Modificare l'account di amministratore

CA ARCserve Central Applications consente di modificare il nome utente e/o la password per l'account dell'amministratore dopo l'installazione dell'applicazione. L'account di amministratore viene utilizzato solo per il nome utente predefinito visualizzato sulla schermata di accesso.

Nota: il nome utente specificato deve essere un account amministrativo di Windows o un account che dispone di privilegi di amministratore di Windows.

Procedere come descritto di seguito:

1. Accedere all'applicazione e fare clic su Configurazione sulla barra di spostamento.

   Vengono visualizzate le opzioni di configurazione.

2. Fare clic su Account di amministratore

3. Vengono visualizzate le impostazioni dell'account di amministratore.

4. Aggiornare i seguenti campi:

   - Nome utente
   - Password

   Fare clic su Salva.

L'account di amministratore viene modificato.

Visualizzazione registri

Il registro attività contiene informazioni complete su tutte le operazioni eseguite dall'applicazione. Il registro fornisce l'itinerario di controllo di ciascun processo eseguito (le attività più recenti vengono elencate in prima posizione) e può essere utile per la risoluzione di eventuali problemi.

Procedere come descritto di seguito:

1. Dalla pagina principale, fare clic su Visualizza registri della barra di navigazione.

   Verrà visualizzata la schermata Visualizza registri.

2. Utilizzare gli elenchi a discesa per specificare le informazioni di registro che si desidera visualizzare.

   - **Gravità** - Consente di specificare la gravità del registro che si desidera visualizzare. È possibile specificare le seguenti opzioni di gravità:
     - **Tutto** - Consente di visualizzare tutti i registri indipendentemente dalla gravità.
     - **Informazioni** - Consente di visualizzare unicamente i registri contenenti informazioni generali.
     - **Errori** - Consente di visualizzare unicamente i registri contenenti la descrizione degli errori gravi che si sono verificati.
     - **Avvisi** - Consente di visualizzare unicamente i registri contenenti la descrizione degli avvisi.
     - **Errori e avvisi** - Consente di visualizzare unicamente i registri di contenenti la descrizione degli errori gravi e di avviso che si sono verificati.
   - **Modulo** - Consente di specificare il modulo di cui si desiderano visualizzare i registri. È possibile specificare le seguenti opzioni di modulo:
     - **Tutto** - Consente di visualizzare i registri relativi a tutti i componenti dell'applicazione.
     - **Comune** - Consente di visualizzare i registri relativi ai processi comuni.
     - **Importa nodi da file** - Consente di visualizzare unicamente i registri relativi al processo di importazione dei nodi nell'applicazione a partire da un file.
     - **Gestione criterio** - Consente di visualizzare unicamente i registri relativi alla gestione dei criteri.
     - **Aggiornamenti** - Consente di visualizzare unicamente i registri relativi all'aggiornamento dell'applicazione.
     - **Sospendi/Riprendi heartbeat** - Consente di visualizzare unicamente i registri dei computer virtuali di standby virtuale il cui heartbeat è stato interrotto o ripreso.

  - **Sospendi/Riprendi Virtual Standby** - Consente di visualizzare unicamente i registri dei computer virtuali di standby virtuale il cui processo di virtual standby è stato interrotto o ripreso.
  - **Aggiorna nodi multipli** - Consente di visualizzare unicamente i registri relativi all'aggiornamento simultaneo di più nodi.
  - **Computer virtuale di standby** - Consente di visualizzare unicamente i registri dei computer virtuali attivati.
  - **Importazione dei nodi da CA ARCserve Replication** - Consente di visualizzare unicamente i registri relativi ai nodi importati da CA ARCserve Replication.

- **Nome nodo** - Consente di visualizzare unicamente i registri relativi a un nodo specifico.

  Nota: questo campo supporta l'uso dei caratteri jolly '*' e '?'. Ad esempio, immettere 'lod*' per visualizzare tutti i registri attività per i computer il cui nome inizia per 'lod'.

Nota: è possibile applicare contemporaneamente le opzioni Gravità, Modulo e Nome nodo. Ad esempio, è possibile visualizzare Errori (Gravità) relativi agli Aggiornamenti (Modulo) per il Nodo X (Nome nodo).

Fare clic su Aggiorna. 

La visualizzazione dei registri dipende dalle opzioni di visualizzazione specificate.

Nota: l'ora visualizzata nel registro dipende dal fuso orario del server di database dell'applicazione.

Aggiungere collegamenti alla barra di spostamento

Per ogni applicazione CA ARCserve Central Applications è presente un collegamento Scheda Aggiungi nuovo sulla barra di navigazione. Questa funzionalità consente di aggiungere voci alla barra di navigazione per le ulteriori applicazioni Web che si desidera gestire. Tuttavia, per ciascuna applicazione installata, verrà aggiunto automaticamente un nuovo collegamento alla barra di navigazione. Ad esempio, se CA ARCserve Central Reporting e CA ARCserve Central Virtual Standby sono stati installati su un Computer A e CA ARCserve Central Reporting viene avviato, CA ARCserve Central Virtual Standby verrà aggiunto automaticamente alla barra di navigazione.

Nota: le applicazioni installate verranno rilevate soltanto se sono presenti altre istanze CA ARCserve Central Applications sullo stesso computer.

Procedere come descritto di seguito:

1. Dalla barra di navigazione dell'applicazione, fare clic sul collegamento Scheda Aggiungi nuovo.
2. Specificare il nome e l'URL per l'applicazione o il sito Web che si desidera aggiungere. Ad esempio, www.google.com.

   Facoltativamente, specificare il percorso di un'icona.
3. Fare clic su OK.

   La nuova scheda viene aggiunta nella parte inferiore della barra di navigazione.

Tenere presenti le seguenti considerazioni:

- Il collegamento al Supporto tecnico di CA viene aggiunto per impostazione predefinita.

  Per rimuovere la nuova scheda, evidenziare la scheda e fare clic sul collegamento Rimuovi.

Pagina principale di Virtual Standby

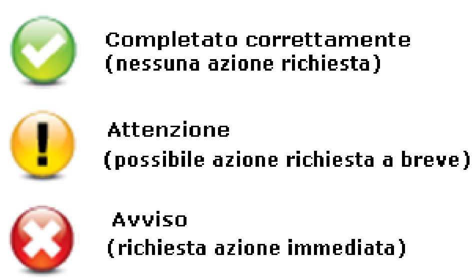
La scheda Virtual Standby sul server di monitoraggio consente di visualizzare informazioni relative a tutti i server CA ARCserve D2D protetti. La scheda Virtual Standby sui server di origine, invece, consente di visualizzare solo le informazioni sul server di origine al quale si esegue l'accesso.

In questa sezione verranno presentati i seguenti argomenti:

Modalità di utilizzo della schermata Riepilogo Virtual Standby

La schermata Riepilogo Virtual Standby contiene diverse icone che forniscono un'indicazione visiva sullo stato corrente delle attività ed indicano il livello di urgenza delle azioni da intraprendere.

La pagina principale contiene le seguenti icone:



La schermata Riepilogo Virtual Standby contiene le seguenti informazioni:

- **Elenco server** - Visualizza un elenco dei server di origine protetti da questo server di monitoraggio. L'elenco ordina i server in base al loro stato corrente. Ad esempio, Tutti, Richiede azione, Server in esecuzione, ecc.

  Nota: gli elenchi di server vengono visualizzati solo se si è connessi al server di monitoraggio. Per ulteriori informazioni, consultare la sezione Modalità di utilizzo dell'elenco server (a pagina 87).

- **Riepilogo Virtual Standby** - Visualizza informazioni di riepilogo per il server di origine selezionato. Per ulteriori informazioni, consultare la sezione Monitoraggio di stato dei processi di conversione virtuale (a pagina 89).

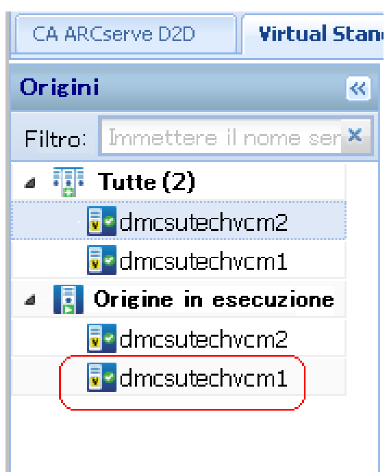
- **Impostazioni di standby virtuale** - Visualizza informazioni di riepilogo sulle impostazioni di conversione virtuale per il server di origine selezionato. Per ulteriori informazioni, consultare la sezione Visualizzazione delle impostazioni di Virtual Standby per i server di origine (a pagina 90).
- **Snapshot del punto di ripristino** - Visualizza un elenco di snapshot del punto di ripristino disponibili per il server di origine selezionato. Per ulteriori informazioni,consultare la sezione Visualizzazione dell'elenco di snapshot del punto di ripristino (a pagina 91).
- **Attività** - Visualizza un elenco di attività che è possibile eseguire per il server di origine selezionato. Per ulteriori informazioni, consultare la sezione Attività di monitoraggio di Virtual Standby (a pagina 91).
- **Accesso al Supporto tecnico e alla community** - Fornisce un meccanismo che consente di inizializzare funzioni relative al supporto.

  Nota: per ulteriori informazioni sull'accesso al Supporto tecnico e alla community, consultare la documentazione di CA ARCserve D2D.

Modalità di utilizzo dell'elenco server

Nell'elenco dei server della schermata Riepilogo Virtual Standby sono riportati i server di origine protetti da un server di monitoraggio. L'elenco ordina i server in base al loro stato corrente. Ad esempio, Tutti, Richiede azione, Origine in esecuzione e così via.

Per eseguire attività di manutenzione o visualizzare informazioni relative a un nodo di CA ARCserve D2D, fare clic sulla scheda Virtual Standby, quindi sul server, come illustrato nella seguente schermata:



Visualizzazione delle informazioni di riepilogo sul processo di standby virtuale più recente

La schermata Nodo consente di visualizzare le informazioni di riepilogo relative al processo di standby virtuale (conversione) più recente per un nodo. È possibile visualizzare le informazioni sui processi di standby virtuale completati correttamente e non riusciti.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby.

   Nella barra di navigazione, fare clic su Nodo per visualizzare la schermata corrispondente.

2. Nella colonna Stato, posizionare il puntatore del mouse su una delle icone seguenti:

   Completato correttamente

   Avviso

   Errore/Non riuscito

   Verrà visualizzata la finestra di messaggio Riepilogo stato del nodo contenente i seguenti risultati relativi al processo di standby virtuale più recente completato:

   Standby virtuale più recente

   Indica la data e l'ora dell'ultimo processo di standby virtuale completato (correttamente o con errori).

   Snapshot del punto di ripristino

   Visualizza il numero di punti di ripristino convertiti per il nodo a partire dal processo Virtual Standby più recente.

   Stato destinazione

   Visualizza lo spazio libero su disco sulla destinazione Virtual Standby. La destinazione può essere:

   - Un archivio dati server ESX utilizzato per la conversione a un sistema server ESX.
   - Spazio libero su disco sul volume in cui il server Hyper-V archivia le snapshot dei punti di ripristino.

3. Spostare il puntatore del mouse dall'icona Stato per chiudere la finestra di messaggio Riepilogo stato del nodo.
4. I campi riportati di seguito contengono ulteriori informazioni sull'ultimo processo di standby virtuale completato correttamente o non riuscito:

   Risultati ultima conversione

   Risultati dell'ultimo processo di standby virtuale completato correttamente o non riuscito. Ad esempio: Completato, Annullato, Non riuscito.

   Data/Ora ultima conversione

   Indica la data e l'ora dell'ultimo processo di standby virtuale completato correttamente o non riuscito.

Verifica dello stato dei processi di conversione virtuale

Virtual Standby consente di monitorare lo stato dei processi di conversione virtuale in corso, nonché di visualizzare informazioni di riepilogo sui dati di conversione virtuale e sui computer virtuali che proteggono i server di origine di CA ARCserve D2D.

Per controllare lo stato di processi di conversione virtuali

1. Aprire Virtual Standby e fare clic su Nodi sulla barra di spostamento.

   Verrà visualizzata la schermata Nodo.
2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.
3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   CA ARCserve D2D viene aperto.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

4. Fare clic sulla scheda Virtual Standby.

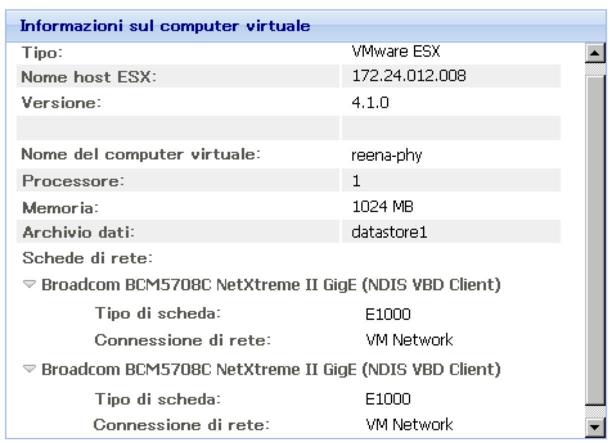
   (Facoltativo) Se il server CA ARCserve D2D è un server di monitoraggio, fare clic sull'elenco dei server, espandere Tutto, Origine in esecuzione o Richiede azione e fare clic sul server che si desidera controllare.

   Virtual Standby visualizza informazioni sui processi di conversione virtuale in corso, informazioni di riepilogo sui processi di conversione virtuali e sul computer virtuale che protegge il server.



Visualizzazione delle impostazioni di Virtual Standby per i server di origine

Nella schermata Riepilogo Virtual Standby vengono visualizzate informazioni sui computer virtuali che proteggono i server di origine.

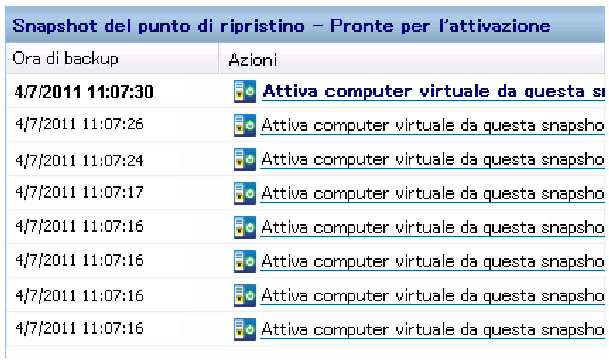


Visualizzazione dell'elenco di snapshot del punto di ripristino

Nella schermata Virtual Standby viene visualizzato un elenco delle snapshot più recenti del punto di ripristino.

La casella di riepilogo visualizza la data e l'ora di completamento del backup del server di CA ARCserve D2D.

Dall'elenco di snapshot del punto di ripristino è possibile attivare i computer virtuali. Per ulteriori informazioni, consultare la sezione Attivazione di snapshot del punto di ripristino.



Snapshot del punto di ripristino – Pronte per l'attivazione

Ora di backup	Azioni
4/7/2011 11:07:30	**Attiva computer virtuale da questa s**
4/7/2011 11:07:26	Attiva computer virtuale da questa snapsho
4/7/2011 11:07:24	Attiva computer virtuale da questa snapsho
4/7/2011 11:07:17	Attiva computer virtuale da questa snapsho
4/7/2011 11:07:16	Attiva computer virtuale da questa snapsho
4/7/2011 11:07:16	Attiva computer virtuale da questa snapsho
4/7/2011 11:07:16	Attiva computer virtuale da questa snapsho
4/7/2011 11:07:16	Attiva computer virtuale da questa snapsho

Nota: se la destinazione Virtual Standby corrisponde a un server VMWare ESX, il numero massimo di snapshot del punto di ripristino visualizzate è pari a 29. Se la destinazione Virtual Standby corrisponde a un server Microsoft Hyper-V Server, il numero massimo di snapshot del punto di ripristino visualizzate è pari a 24.

Attività di monitoraggio di CA ARCserve Central Virtual Standby

Virtual Standby consente di eseguire le seguenti attività di monitoraggio:

- Sospendere e riprendere heartbeat.
- Sospendere e riprendere processi Virtual Standby.
- Visualizzare i dati del registro attività su conversioni virtuali e snapshot del punto di ripristino (a pagina 92).
- Attivare snapshot del punto di ripristino.

Visualizzazione dei dati di processo del registro attività

Virtual Standby consente di visualizzare le informazioni del registro attività sui processi di conversione virtuale. Il registro attività contiene record del processo di conversione virtuale per i server di origine di CA ARCserve D2D protetti.

Nota: il registro attività (activity.log) viene archiviato sul server di installazione di CA ARCserve D2D nella seguente directory:

```
C:\Program Files\CA\ARCserve D2D\Logs
```

Per visualizzare dati di processo del registro delle attività

1. Aprire Virtual Standby e fare clic su Nodi sulla barra di spostamento.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   CA ARCserve D2D viene aperto.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

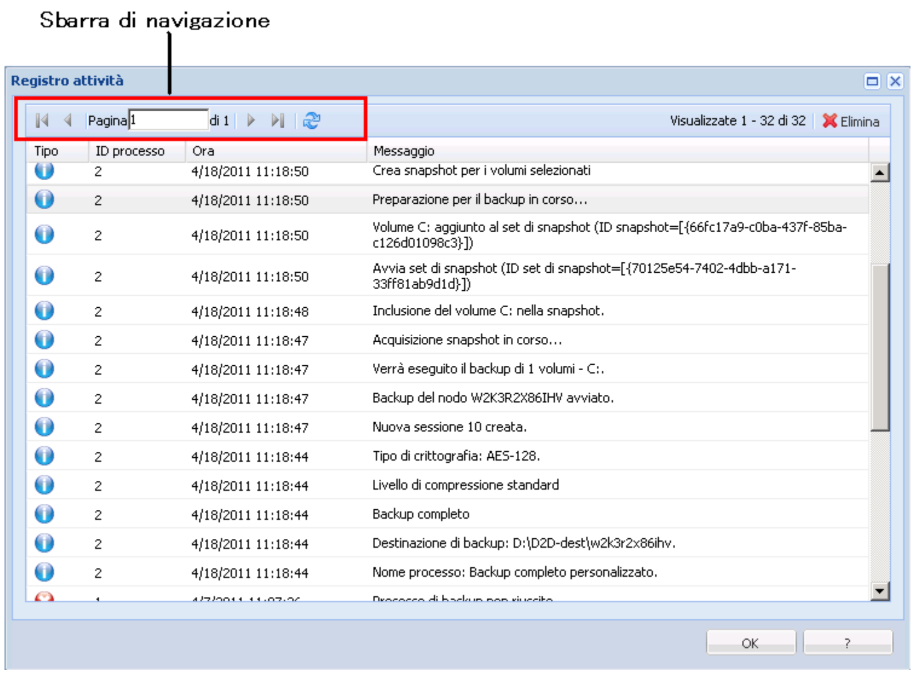
4. Fare clic sulla scheda Virtual Standby.

   Verrà visualizzata la schermata Riepilogo Virtual Standby.

5. (Facoltativo) Se l'utente è connesso al server di monitoraggio, espandere Tutto o In esecuzione dall'elenco Server, quindi fare clic sul nodo di cui si desidera visualizzare i dati del Registro attività.

   Dall'elenco delle attività di conversione virtuale situato nella parte destra della schermata Riepilogo Virtual Standby, fare clic su Visualizza registri.

   Viene visualizzata la finestra di dialogo Registro attività.



   Utilizzare la barra di spostamento per cercare e visualizzare i record del registro attività. Nel registro attività vengono visualizzate le seguenti icone:

    Informazioni

    Avviso

    Errore

   Nota: per informazioni sull'eliminazione dei record di registro delle attività, consultare la sezione Eliminazione dei record del registro attività (a pagina 94).

Eliminazione dei record del Registro attività

Virtual Standby consente di gestire i dati del registro attività nel loro insieme. Il Registro attività contiene record di processo per i nodi di origine di CA ARCserve D2D protetti. Se si esegue la protezione di un numero elevato di server di origine o vengono eseguiti backup frequenti, il Registro attività potrebbe occupare una quantità elevata di spazio su disco sul nodo CA ARCserve D2D.

Pertanto, è possibile eliminare record del registro attività antecedenti ad una determinata data oppure cancellare tutti i record del registro attività.

Nota: il registro attività (activity.log) viene archiviato sul server di installazione di CA ARCserve D2D nella seguente directory:

```
C:\Program Files\CA\ARCserve D2D\Logs
```

Per eliminare i record del Registro attività

1. Aprire Virtual Standby e fare clic su Nodi sulla barra di spostamento.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   CA ARCserve D2D viene aperto.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

4. Fare clic sulla scheda Virtual Standby.

   Verrà visualizzata la schermata Riepilogo Virtual Standby.

5. (Facoltativo) Se l'utente è connesso al server di monitoraggio, espandere Tutto o In esecuzione dall'elenco Server, quindi fare clic sul nodo di cui si desiderano eliminare i dati del Registro attività.

6. Dall'elenco delle attività di conversione virtuale situato nella parte destra della schermata Riepilogo Virtual Standby, fare clic su Visualizza registri.

   Viene visualizzata la finestra di dialogo Registro attività.

7. Fare clic su Elimina della barra degli strumenti.

   Verrà visualizzata la finestra di dialogo Eliminazione registro attività.

8. Selezionare una delle seguenti opzioni:

   - **Elimina tutti i record di registro** - Consente di eliminare tutti i record di processo del registro attività.

     Nota: prestare la massima attenzione con l'utilizzo di questa opzione. Se i record del registro attività vengono eliminati, non sarà più possibile recuperarli.

   - **Elimina tutti i record di registro antecedenti al** - Consente di cancellare tutti i record del registro attività antecedenti alla data specificata.

   Fare clic su OK.

I record vengono eliminati dal registro attività.

Visualizzazione delle informazioni di stato sui processi di standby virtuale dal server Virtual Standby

CA ARCserve Central Virtual Standby converte i punti di ripristino di CA ARCserve D2D in snapshot del punto di ripristino. È possibile visualizzare le informazioni di stato relative ai processi di standby virtuale in corso.

Se lo si desidera, è possibile accedere alle informazioni di stato dal server Virtual Standby o direttamente dal nodo. Per informazioni sulla visualizzazione delle informazioni di stato dai nodi, consultare la sezione Visualizzazione delle informazioni di stato sui processi di standby virtuale dai nodi (a pagina 96).

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby.

   Nella barra di navigazione, fare clic su Nodo per visualizzare la schermata corrispondente.

2. Se sono presenti processi di standby virtuale in corso, la fase del processo viene visualizzata nel campo Processo, come illustrato nell'immagine seguente:

	Nome nodo	Criterio	Nome del comput...	vCenter/ESX	Processo
☑	w2k3r2x86jvp1	Nuovo criterio	W2K3R2x86Jvp1	155.35.128.119	Avvio in corso...

3. Fare clic sulla fase per aprire la finestra di dialogo Monitor di stato di Virtual Standby.

   Nota: per informazioni sui campi visualizzati in Monitor di stato di Virtual Standby, consultare la sezione Monitor di stato di Virtual Standby (a pagina 97).

4. Fare clic su Chiudi per chiudere la finestra di dialogo Monitor di stato di Virtual Standby.

Visualizzazione delle informazioni di stato dei processi di standby virtuale dai nodi

CA ARCserve Central Virtual Standby converte i punti di ripristino di CA ARCserve D2D in snapshot del punto di ripristino. È possibile visualizzare le informazioni di stato sui processi di conversione in corso.

Se lo si desidera, è possibile accedere alle informazioni di stato dal server Virtual Standby o direttamente dal nodo. Per informazioni sulla visualizzazione delle informazioni di stato dal server Virtual Standby, consultare la sezione Visualizzazione delle informazioni di stato sui processi di standby virtuale dal server Virtual Standby (a pagina 95).

Procedere come descritto di seguito:

1. Aprire l'applicazione e fare clic su Nodi sulla barra di navigazione.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

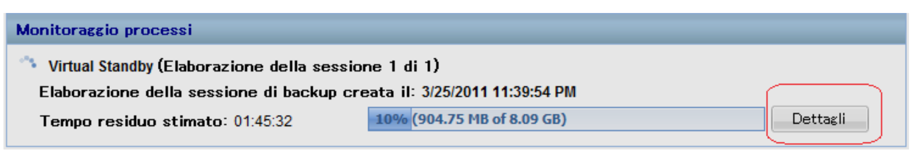
   L'utente è connesso al nodo CA ARCserve D2D.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

4. Fare clic sulla scheda Virtual Standby.

   Verrà visualizzata la schermata Riepilogo Virtual Standby.

   Nel caso in cui sia presente un processo di standby virtuale in corso, verrà visualizzata una finestra di stato nel campo Monitoraggio processi, come illustrato nell'immagine seguente:

5. Fare clic su Dettagli per accedere a Monitor di stato di Virtual Standby.

   Nota: per informazioni sui campi visualizzati in Monitor di stato di Virtual Standby, consultare la sezione Monitor di stato di Virtual Standby (a pagina 97).

6. Fare clic su Chiudi per chiudere la finestra di dialogo Monitor di stato di Virtual Standby.

Monitor di stato di Virtual Standby

Il Monitor di stato di Virtual Standby visualizza le seguenti informazioni in tempo reale relative al processo di standby virtuale:

Fase

Visualizza la fase corrente del processo di conversione.

Annulla processo

Consente di terminare il processo di conversione.

Elaborazione in corso

Visualizza l'avanzamento generale del processo di conversione e il numero di sessione del punto di ripristino in corso di conversione.

Punto di provisioning corrente

Visualizza le informazioni di stato sulla sessione in corso di conversione.

Sessioni di origine

Specifica il numero di sessioni in corso di conversione.

Ora inizio

Visualizza la data e l'ora di inizio della conversione della sessione.

Tempo trascorso

Visualizza il tempo trascorso dall'avvio della conversione della sessione corrente.

Velocità effettiva

Visualizza la velocità di conversione della sessione.

Tempo residuo stimato

Visualizza il tempo stimato restante per la conversione della sessione di origine corrente.

Tutte le sessioni

Visualizza le informazioni di stato relative a tutte le sessioni del punto di ripristino in corso di conversione.

Numero di sessioni convertite

Visualizza il numero totale di sessioni convertite del punto di provisioning.

Tempo trascorso

Visualizza il tempo trascorso dall'avvio della conversione di tutte le sessioni contenute nel punto di ripristino.

Tempo residuo stimato

Visualizza il tempo stimato restante per la conversione di tutte le sessioni contenute nel punto di ripristino.

Numero di sessioni in sospeso

Visualizza il numero di sessioni in attesa di conversione.

Visualizzare informazioni sui criteri assegnati ai nodi di CA ARCserve D2D

L'applicazione consente di visualizzare informazioni sui criteri di conversione assegnati ai nodi di CA ARCserve D2D.

Per visualizzare informazioni sui criteri assegnati ai nodi di CA ARCserve D2D

1. Aprire l'applicazione e fare clic su Nodi sulla barra di spostamento.

   Verrà visualizzata la schermata Nodo.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare e fare clic sul nodo a cui si desidera accedere, quindi su Accesso a D2D dal menu di scelta rapida.

   L'utente è connesso al nodo CA ARCserve D2D.

   Nota: se non viene aperta una nuova finestra, verificare che le opzioni del browser non blocchino la visualizzazione di tutti i popup o di quelli del sito Web corrente.

4. Fare clic sulla scheda Virtual Standby.

   Verrà visualizzata la schermata Riepilogo Virtual Standby.

5. Dall'elenco Attività Virtual Standby, fare clic su Impostazioni Virtual Standby.

   Verrà visualizzata la finestra di dialogo Impostazioni Virtual Standby.

   La finestra di dialogo Impostazioni Virtual Standby consente di visualizzare le informazioni relative al server di virtualizzazione, al computer virtuale, al server di sostituzione e alle preferenze definite nel criterio assegnato al nodo di CA ARCserve D2D. Non è possibile modificare i criteri assegnati a CA ARCserve D2D dalla finestra di dialogo Impostazioni Virtual Standby.

   Nota: per informazioni su come modificare i criteri, consultare la sezione Modifica dei criteri.

6. Fare clic su Annulla per chiudere la finestra di dialogo Impostazioni Virtual Standby.

Impostazioni di standby virtuale

La finestra di dialogo Impostazioni di standby virtuale contiene informazioni sul criterio assegnato al nodo. Non è possibile modificare i criteri da questa finestra di dialogo. Per ulteriori informazioni, consultare la sezione Modifica dei criteri.

Nella scheda Standby virtuale sono presenti le opzioni riportate di seguito:

Opzioni del server di virtualizzazione

- **Sistemi VMware**

  Le opzioni seguenti sono valide per i sistemi VMware:

  - **Tipo di virtualizzazione:** VMware.
  - **Host ESX/vCenter:** identifica il nome host del sistema ESX o vCenter Server.
  - **Nome utente**: identifica il nome utente per l'accesso al sistema VMware.
  - **Password**: identifica la password associata al nome utente per l'accesso al sistema VMware.
  - **Protocollo:** visualizza il protocollo di comunicazione utilizzato tra il nodo CA ARCserve D2D di origine e il server di monitoraggio.
  - **Porta:** identifica la porta utilizzata per il trasferimento di dati tra il server di origine e il server di monitoraggio.

- **Monitoraggio:**

  Le opzioni seguenti sono valide per i sistemi VMware.

  - **Server di monitoraggio:** identifica il nome host del server che esegue il monitoraggio del server di origine.
  - **Nome utente**: identifica il nome utente per l'accesso al server di monitoraggio.
  - **Password**: identifica la password associata al nome utente per l'accesso al server di monitoraggio.
  - **Protocollo:** identifica il protocollo di comunicazione utilizzato tra il server CA ARCserve Central Virtual Standby e il sistema ESX Server (server di monitoraggio).
  - **Porta:** identifica la porta utilizzata per il trasferimento di dati tra il server CA ARCserve Central Virtual Standby e il sistema ESX Server (server di monitoraggio).
  - **Usa server di monitoraggio come proxy per il trasferimento dei dati**: specifica che il server di monitoraggio copia i dati di conversione dal server di origine CA ARCserve D2D all'archivio dati di ESX Server.

    Nota: l'opzione Usa server di monitoraggio come proxy per il trasferimento dei dati è abilitata per impostazione predefinita. È possibile disattivare questa opzione per consentire al server di origine di CA ARCserve D2D di copiare il dati di conversione direttamente sull'archivio dati del server ESX.

- **Sistemi Hyper-V**

  Le opzioni seguenti sono valide per i sistemi Hyper-V:

  - **Tipo di virtualizzazione:** Hyper-V.
  - **Nome host Hyper-V**: identifica il nome host del sistema Hyper-V.
  - **Nome utente**: identifica il nome utente per l'accesso al sistema Hyper-V.
  - **Password**: identifica la password associata al nome utente per l'accesso al sistema Hyper-V.
  - **Porta:** identifica la porta utilizzata per il trasferimento di dati tra il server di origine e il server di monitoraggio.

Opzioni del computer virtuale

- **Sistemi VMware**
  - **Prefisso nome del computer virtuale:** identifica il nome del computer virtuale sul sistema ESX Server.

    Valore predefinito: CAVM_
  - **Pool di risorse del computer virtuale**: identifica il nome del pool di risorse in cui è raggruppato il computer virtuale di standby.
  - **Archivio dati**: identifica la posizione in cui si desidera archiviare i dati di conversione.
    - **Usa un archivio dati per tutti i dischi di origine del computer virtuale**: indica che l'applicazione copia tutti i dischi correlati al computer virtuale in un unico archivio di dati.
    - **Selezionare un archivio dati per ciascun disco di origine:** indica che l'applicazione copia le informazioni relative al disco per il computer virtuale nell'archivio dati corrispondente.
  - **Reti:** identifica le NIC, le reti virtuali e i percorsi che il sistema ESX Server utilizza per comunicare con i computer virtuali.
    - **Connetti tutte le NIC virtuali alla seguente rete virtuale**: identifica le schede di rete virtuali che sono mappate alla rete virtuale. Questa opzione viene specificata quando il computer virtuale contiene NIC virtuali e una rete virtuale.
    - **Selezionare una rete virtuale per ciascuna scheda di interfaccia di rete virtuale:** identifica il nome della rete virtuale che la NIC deve utilizzare per comunicare.
  - **Conteggio CPU**: identifica il numero minimo e massimo di CPU supportato dal computer virtuale di standby.
  - **Memoria**: identifica la quantità totale di RAM in MB allocata per il computer virtuale di standby.

- **Sistemi Hyper-V**
  - **Prefisso nome del computer virtuale:** identifica il nome del computer virtuale sul sistema Hyper-V.

    Valore predefinito: CAVM_
  - **Percorso:** identifica la posizione sul server Hyper-V in cui sono archiviati i dati di conversione.
  - **Reti:** identifica le NIC, le reti virtuali e i percorsi che il server Hyper-V utilizza per comunicare con i computer virtuali.
  - **Conteggio CPU**: identifica il numero minimo e massimo di CPU supportato dal computer virtuale di standby.
  - **Memoria**: identifica la quantità totale di RAM in MB allocata al computer virtuale di standby.

Impostazioni di sostituzione

- **Recupero:**
  - **Avvia il computer virtuale manualmente**: indica che l'avvio e il provisioning dei computer virtuali vengono eseguiti manualmente quando si verificano errori sul server di origine o la comunicazione viene interrotta.
  - **Avvia il computer virtuale automaticamente**: indica che l'avvio e il provisioning dei computer virtuali vengono eseguiti automaticamente quando si verificano errori sul server di origine o la comunicazione viene interrotta.
- **Proprietà heartbeat:**
  - **Timeout:** indica la durata dell'attesa di un heartbeat da parte del server di monitoraggio prima di attivare la snapshot di un punto di ripristino.
  - **Frequenza:** identifica la frequenza con cui il server di origine comunica gli heartbeat al server di monitoraggio.

Nella scheda Preferenze sono presenti le opzioni riportate di seguito:

- **Avvisi di posta elettronica:**
  - **Heartbeat mancante per il computer di origine**: indica che Virtual Standby invia notifiche di avviso quando il server di monitoraggio non rileva un heartbeat nel server di origine.
  - **Computer virtuale attivo per il computer di origine configurato con attivazione automatica**: indica che Virtual Standby invia notifiche di avviso quando viene attivato un computer virtuale configurato per l'attivazione automatica nel caso in cui l'heartbeat non venga rilevato.

- **Heartbeat mancante per il computer di origine configurato con attivazione manuale**: indica che Virtual Standby invia notifiche di avviso quando non viene rilevato nessun heartbeat da un server di origine non configurato per l'attivazione automatica.
- **Spazio di archiviazione disponibile sul computer virtuale inferiore a**: indica che Virtual Standby invia notifiche di avviso quando viene rilevato spazio su disco insufficiente sul percorso dell'hypervisor definito. Ciò si verifica quando la quantità di spazio disponibile su disco è inferiore alla soglia definita dall'utente. La soglia può essere rappresentata da un valore assoluto (MB) o da una percentuale della capacità del volume.
- **Errori/Arresto anomalo dello standby virtuale:** indica che Virtual Standby invia notifiche di avviso quando si verifica un errore durante il processo di conversione.
- **Virtual Standby eseguito correttamente** - Indica che il processo di creazione di un computer virtuale di standby virtuale è stato completato correttamente.
- **Hypervisor non raggiungibile:** indica che Virtual Standby invia notifiche di avviso quando vengono rilevati errori di comunicazione con il sistema ESX Server o Hyper-V.
- **Errore di licenza**: indica che Virtual Standby invia notifiche di avviso quando vengono rilevati problemi di licenza sui server Virtual Standby, sui server di origine e sui server di monitoraggio.
- **Errore di avvio di Virtual Standby dalla snapshot del punto di ripristino** - Indica che il processo di creazione di un computer virtuale di standby virtuale a partire da una snapshot del punto di ripristino ha prodotto un errore.

Sospensione e riattivazione dei processi di standby virtuale dal server Virtual Standby

La conversione virtuale è il processo in cui Virtual Standby converte i punti di ripristino di CA ARCserve D2D da nodi di origine a file di dati del computer virtuale, denominati snapshot del punto di ripristino. In caso di errore del nodo di origine, Virtual Standby utilizza le snapshot del punto di ripristino per attivare un computer virtuale per il nodo di origine.

Si consiglia di impostare il processo di conversione virtuale per il funzionamento continuo. Ad ogni modo, se si desidera sospendere temporaneamente il processo di conversione virtuale, è possibile procedere alla sospensione dal server Virtual Standby. Dopo aver risolto i problemi relativi al nodo di origine, sarà possibile riprendere il processo di conversione virtuale.

Quando i processi di Virtual Standby (processi di conversione) vengono sospesi, l'operazione di sospensione non sospende il processo di conversione in corso. La sospensione viene eseguita solamente per il processo la cui esecuzione è prevista al completamento del successivo processo di backup di CA ARCserve D2D. Pertanto, il processo di conversione successivo verrà avviato unicamente quando l'utente specifica che desidera riattivare il processo di conversione sospeso.

Nota: se lo si desidera, è possibile sospendere e riattivare i processi di standby virtuale direttamente dai nodi. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi di standby virtuale dai nodi.

Procedere come descritto di seguito:

1. Accedere server di standby virtuale e fare clic su Nodo sulla barra Navigazione per aprire la schermata Nodo.
2. Eseguire una delle azioni seguenti per specificare i processi di standby virtuale che si desidera sospendere o riattivare:
   - **Livello di nodo**: fare clic sul gruppo contenente i nodi che si desidera sospendere o riattivare e selezionare la casella di controllo corrispondente.
   - **Livello di gruppo**: fare clic sul gruppo contenente che si desidera sospendere o riattivare.
3. Eseguire una delle seguenti operazioni:
   - Fare clic su Virtual Standby dalla barra degli strumenti, quindi selezionare Sospendi o Riprendi dal menu di scelta rapida per sospendere temporaneamente i processi di conversione.

Fare clic sul gruppo selezionato oppure sui nodi, quindi selezionare Sospendi Virtual Standby o Riprendi Virtual Standby dal menu di scelta rapida per riprendere i processi di conversione.

Sospensione e ripresa dei processi di stanby virtuale dai nodi

La conversione virtuale è il processo in cui Virtual Standby converte i punti di ripristino di CA ARCserve D2D da nodi di origine a file di dati del computer virtuale, denominati snapshot del punto di ripristino. In caso di errore del nodo di origine, Virtual Standby utilizza le snapshot del punto di ripristino per attivare un computer virtuale per il nodo di origine.

Si consiglia di impostare il processo di conversione virtuale per il funzionamento continuo. Ad ogni modo, se si desidera sospendere temporaneamente il processo di conversione virtuale, è possibile procedere alla sospensione dal server Virtual Standby. Dopo aver risolto i problemi relativi al nodo di origine, sarà possibile riprendere il processo di conversione virtuale.

Quando i processi di Virtual Standby (processi di conversione) vengono sospesi, l'operazione di sospensione non sospende il processo di conversione in corso. La sospensione viene eseguita solamente per il processo la cui esecuzione è prevista al completamento del successivo processo di backup di CA ARCserve D2D. Pertanto, il processo di conversione successivo verrà avviato unicamente quando l'utente specifica che desidera riattivare il processo di conversione sospeso.

Nota: se lo si desidera, è possibile sospendere e riattivare i processi di standby virtuale dal server Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi di standby virtuale dal server Virtual Standby.

Procedere come descritto di seguito:

1. Nella barra di navigazione, fare clic su Virtual Standby, quindi su Nodi per visualizzare la schermata corrispondente.
2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere per visualizzare tutti i nodi associati al gruppo specificato.
3. Individuare e fare clic sul nodo che si desidera sospendere o riattivare, quindi fare clic su Accesso a D2D dal menu di scelta rapida per aprire CA ARCserve D2D.
4. Fare clic sulla scheda Virtual Standby per aprire la schermata Riepilogo Virtual Standby.
5. (Facoltativo) Se l'utente è connesso a un server di monitoraggio, dall'elenco Server espandere le opzioni Tutto o Origine in esecuzione, quindi fare clic sul nodo per il quale si desidera sospendere o riprendere il processo di standby virtuale.

   Nota: se il processo di conversione di Virtual Standby è in esecuzione, verrà visualizzata l'opzione Sospendi Virtual Standby nell'elenco delle attività Virtual Standby. Se il processo di conversione di Virtual Standby non è in esecuzione, verrà visualizzata l'opzione Riprendi Virtual Standby nell'elenco delle attività Virtual Standby.

6. Eseguire una delle seguenti operazioni:
   - Fare clic su Sospendi Virtual Standby per sospendere temporaneamente i processi di conversione.

Fare clic su Riprendi Virtual Standby per riattivare i processi di conversione.

Sospensione e riattivazione degli heartbeat dal server Virtual Standby

Virtual Standby consente di sospendere e riprendere gli heartbeat rilevati dal server di monitoraggio. L'heartbeat è il processo utilizzato per la comunicazione dello stato del server di origine tra il server di origine e il server di monitoraggio. Se il server di monitoraggio non rileva alcun heartbeat dopo un periodo di tempo specificato, Virtual Standby può attivare il computer virtuale affinché funzioni come nodo di origine.

Esempi: Sospensione e riattivazione degli heartbeat

Gli esempi riportati di seguito descrivono i casi che richiedono la sospensione e la riattivazione degli heartbeat:

- Sospendere l'heartbeat se si desidera modificare lo stato del nodo in Non in linea (server di origine) per eseguire operazioni di manutenzione.
- Riattivare l'heartbeat dopo aver completato le attività di manutenzione. Lo stato del nodo (server di origine) è in linea.

Tenere presenti le seguenti considerazioni:

- È possibile sospendere e riattivare gli heartbeat a livello di gruppo o di nodo singolo.
- È possibile sospendere e riattivare gli heartbeat per uno o più nodi in una fase.
- In caso di interruzione dell'heartbeat, CA ARCserve Central Virtual Standby non attiva le snapshot del punto di ripristino.
- Durante l'aggiornamento delle installazioni di CA ARCserve D2D sui nodi di origine, CA ARCserve Central Virtual Standby sospende l'heartbeat per i nodi. Per garantire che i server di monitoraggio controllino i nodi aggiornati, riattivare l'heartbeat per i nodi, una volta completato l'aggiornamento.

Nota: se lo si desidera, è possibile sospendere o riattivare gli heartbeat sul nodo dalla schermata Riepilogo Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione degli heartbeat dai nodi.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby.

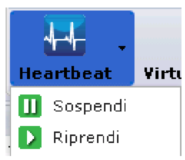
   Nella barra di navigazione, fare clic su Nodo per visualizzare la schermata corrispondente.

2. Eseguire una delle azioni seguenti per specificare i nodi che si desidera sospendere o riattivare:

   - **Livello di nodo**: fare clic sul gruppo contenente i nodi che si desidera sospendere o riattivare e selezionare la casella di controllo corrispondente.
   - **Livello di gruppo**: fare clic sul gruppo contenente che si desidera sospendere o riattivare.

3. Effettuare una delle azioni seguenti per sospendere o riattivare l'heartbeat:

   - Fare clic su Heartbeat della barra degli strumenti e selezionare Sospendi o Riprendi dal menu di scelta rapida, come illustrato nella seguente schermata:



   - Fare clic con il tasto destro del mouse sul gruppo selezionato oppure sui nodi, quindi selezionare Sospendi hearbeat o Riprendi heartbeat dal menu di scelta rapida, come illustrato nella seguente schermata:



Sospensione e ripresa di hearbeat dai nodi

Virtual Standby consente di sospendere e riprendere gli heartbeat rilevati dal server di monitoraggio. L'heartbeat è il processo utilizzato per la comunicazione dello stato del server di origine tra il server di origine e il server di monitoraggio. Se il server di monitoraggio non rileva alcun heartbeat dopo un periodo di tempo specificato, Virtual Standby può attivare il computer virtuale affinché funzioni come nodo di origine.

Esempi: Sospensione e riattivazione degli heartbeat

Gli esempi riportati di seguito descrivono i casi che richiedono la sospensione e la riattivazione degli heartbeat:

- Sospendere l'heartbeat se si desidera modificare lo stato del nodo in Non in linea (server di origine) per eseguire operazioni di manutenzione.
- Riattivare l'heartbeat dopo aver completato le attività di manutenzione. Lo stato del nodo (server di origine) è in linea.

Nota: se lo si desidera, è possibile sospendere e riattivare gli heartbeat dalla schermata Nodo del server Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione degli heartbeat dal server Virtual Standby.

Procedere come descritto di seguito:

1. Accedere al server Virtual Standby.

   Nella barra di navigazione, fare clic su Nodo per visualizzare la schermata corrispondente.

2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Individuare a e fare clic sul nodo per il quale si desidera sospendere o riprendere l'heartbeat e fare clic su Accesso a D2D dal menu di scelta rapida.

   CA ARCserve D2D viene aperto.

4. Fare clic sulla scheda Virtual Standby.

   Verrà visualizzata la schermata Riepilogo Virtual Standby.

5. (Facoltativo) Se l'utente è connesso al server di monitoraggio, espandere Tutto o In esecuzione dall'elenco Server, quindi fare clic sul nodo di cui si desidera sospendere o riprendere l'heartbeat.

   Nota: se l'heartbeat è in esecuzione, l'opzione Sospendi heartbeat verrà visualizzata nell'elenco di attività Conversione virtuale. Se l'heartbeat non è in esecuzione, verrà visualizzata l'opzione Riprendi heartbeat nell'elenco delle attività di conversione virtuale.

6. Eseguire una delle seguenti operazioni:
   - Se l'heartbeat è in esecuzione, fare clic su Sospendi heartbeat per sospendere temporaneamente l'heartbeat.

     Esempio: l'utente desidera utilizzare il server in modalità non in linea per eseguire attività di manutenzione.
   - Se l'heartbeat non è in esecuzione (è stato sospeso), fare clic su Riprendi heartbeat per riprendere l'heartbeat.

     Esempio: le attività di manutenzione sono state completate e si desidera utilizzare il server in modalità in linea.

L'heartbeat viene sospeso o riattivato.

Modifica del protocollo di comunicazione del server

Per impostazione predefinita, CA ARCserve Central Applications utilizza il protocollo HTTP (Hypertext Transfer Protocol) per la comunicazione tra i componenti. Se si desidera utilizzare un livello di protezione superiore per la comunicazione delle password tra i componenti, è possibile utilizzare il protocollo HTTPS (Hypertext Transfer Protocol Secure). Se non si desidera utilizzare tale livello di protezione aggiuntivo, è possibile modificare il protocollo utilizzato selezionando HTTP.

Procedere come descritto di seguito:

1. Accedere al computer di installazione dell'applicazione utilizzando un account amministrativo o un account con privilegi di amministratore.

   Nota: se l'accesso non viene eseguito con un account amministrativo o un con privilegi di amministratore, sarà necessario configurare la riga di comando per l'esecuzione con privilegi di amministratore.
2. Aprire la riga di comando di Windows.

3. Eseguire una delle seguenti operazioni:

   - **Per modificare il protocollo da HTTP a HTTPS:**

     Avviare l'utilità "changeToHttps.bat" dal percorso predefinito riportato di seguito (la posizione della cartella BIN può variare in base al percorso di installazione dell'applicazione):

     ```
     C:\Programmi\CA\ARCserve Central Applications\BIN
     ```

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     ```
     Il protocollo di comunicazione è stato convertito in HTTPS.
     ```

   - **Per modificare il protocollo da HTTPS a HTTP:**

     Avviare l'utilità "changeToHttp.bat" dal percorso predefinito riportato di seguito (la posizione della cartella BIN può variare in base al percorso di installazione dell'applicazione):

     ```
     C:\Programmi\CA\ARCserve Central Applications\BIN
     ```

     Una volta apportate le modifiche al protocollo, verrà visualizzato il messaggio seguente:

     ```
     Il protocollo di comunicazione è stato convertito in HTTP.
     ```

4. Riavviare il browser e connettersi nuovamente a CA ARCserve Central Applications.

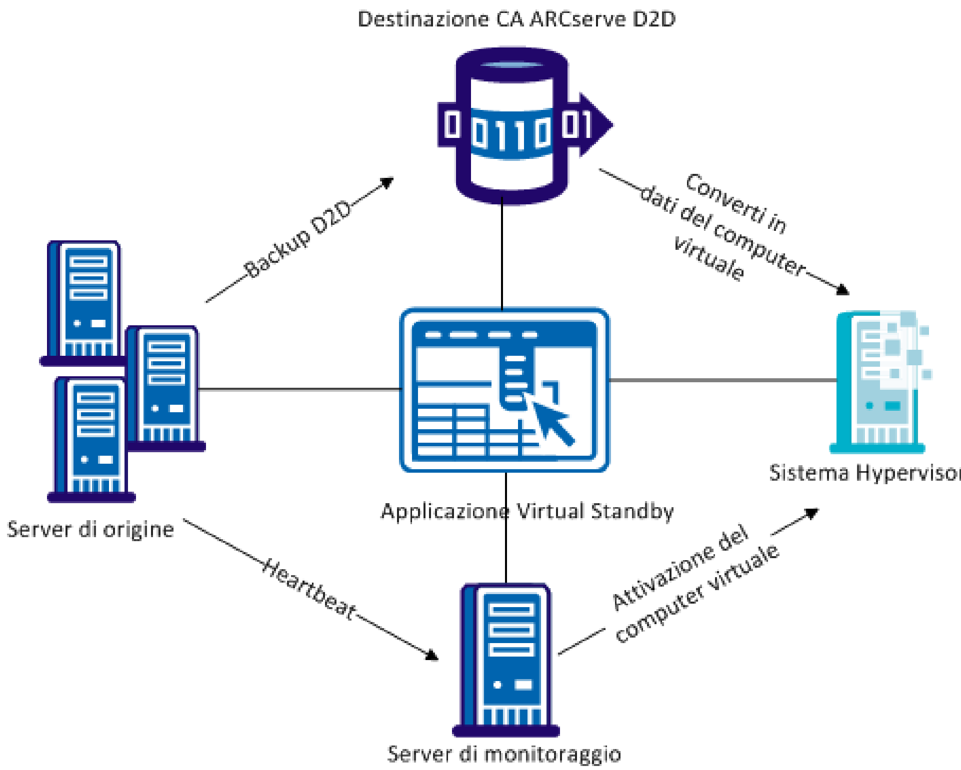
   Nota: in caso di modifica del protocollo in HTTPS, verrà visualizzato un avviso nel browser Web. Questo comportamento è causato da un certificato di protezione autofirmato che richiede all'utente di ignorare l'avviso e continuare oppure di aggiungere il certificato al browser per evitarne la visualizzazione.

Capitolo 6: Attivazione dei computer virtuali di Virtual Standby

Questa sezione contiene i seguenti argomenti:

Attivazione dei computer virtuali locali di Virtual Standby

Questo scenario descrive le procedure utilizzate dai manager dell'archiviazione per sospendere e riprendere gli heartbeat dal server di standby virtuale, sospendere e riprendere il processo di conversione virtuale dal server di standby virtuale, attivare automaticamente i computer di standby virtuale e proteggere i computer virtuali dopo l'attivazione.



La tabella seguente riporta le sezioni che descrivono le attività di attivazione dei computer di standby virtuale:

Attività	Sezione
Attivare automaticamente i computer virtuali di standby virtuale da snapshot del punto di ripristino quando il server di monitoraggio non è in grado di rilevare heartbeat dal server di origine.	Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino (a pagina 112)
Proteggere i computer virtuali di standby virtuale dopo l'attivazione dei computer virtuali.	Protezione dei computer virtuali di Virtual Standby dopo l'attivazione (a pagina 116)

Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino

Virtual Standby può essere configurato in modo tale da attivare computer virtuali Virtual Standby a partire da snapshot del punto di ripristino quando il server di monitoraggio non rileva heartbeat dal server di origine. In alternativa, è possibile attivare computer virtuali Virtual Standby dalle snapshot del punto di ripristino manualmente in caso di errore del server di origine, in caso di emergenza oppure se si desidera utilizzare un server di origine in modalità non in linea per la manutenzione.

Nota: le operazioni riportate di seguito descrivono come attivare computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino manualmente. Per informazioni sulla configurazione di Virtual Standby per l'attivazione automatica delle snapshot del punto di ripristino, consultare la sezione Creazione dei criteri CA ARCserve Central Virtual Standby (a pagina 40).

Procedere come descritto di seguito:

1. Nella barra di navigazione, fare clic su Virtual Standby, quindi su Nodi per visualizzare la schermata corrispondente.
2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.

3. Cercare e selezionare il nodo che si desidera attivare da una snapshot del punto di ripristino, quindi selezionare Computer virtuale di standby dalla barra degli strumenti Azioni.

   Verrà visualizzata la finestra di dialogo Snapshot del punto di ripristino.

4. Nella finestra di dialogo Snapshot del punto di ripristino, eseguire una delle operazioni seguenti:

   - Selezionare un intervallo di tempo della snapshot del punto di ripristino per l'attivazione del computer virtuale.

   OPPURE

   - Selezionare la casella di controllo Attivare il computer di standby virtuale con configurazioni di rete personalizzate per aprire la finestra di dialogo Configurazione di rete del computer virtuale di standby.

     Nota: se il computer virtuale di standby non è ancora stato configurato, verrà visualizzato il collegamento: La rete del computer virtuale di standby non è configurata. Fare clic su questo collegamento per configurare la rete.

   Fare clic su Salva. Le impostazioni vengono salvate per il computer virtuale di standby virtuale.

   Fare clic su Chiudi. Viene visualizzata la finestra di dialogo Snapshot del punto di ripristino.

   Fare clic su Attiva computer virtuale.

Il computer virtuale viene attivato utilizzando i dati contenuti nella snapshot del punto di ripristino.

Nota: dopo l'attivazione del computer virtuale è possibile che venga chiesto di riavviare il computer una o più volte. Ciò si verifica se VMware installa gli strumenti VMware o Windows Hyper-V installa i servizi di integrazione sul computer virtuale.

Dopo l'attivazione di computer virtuali Virtual Standby dalle snapshot del punto di ripristino, potrebbe essere necessario effettuare le seguenti attività:

- Attivare il sistema operativo di Windows in esecuzione sul computer virtuale.
- Avviare i backup di CA ARCserve D2D sul computer virtuale.

  Nota: per informazioni sulla creazione e l'assegnazione di criteri di backup di CA ARCserve D2D mediante CA ARCserve Central Protection Manager, consultare la *Guida per l'utente di CA ARCserve Central Protection Manager.*

- Aggiornare CA ARCserve Central Virtual Standby con il nome host, l'indirizzo IP, e le credenziali di accesso per il computer virtuale.
- Assegnare il nodo a un criterio.

Nota: questa attività è richiesta solo se si desidera creare snapshot del punto di ripristino per il computer virtuale attivo. Per ulteriori informazioni, consultare la sezione Assegnazione dei nodi a un criterio (a pagina 53).

Attivazione di computer virtuali Virtual Standby dalla Gestione Hyper-V

Se si desidera attivare manualmente computer virtuali Virtual Standby, si consiglia di eseguire tale procedura dalla schermata Virtual Standby del server CA ARCserve D2D. Per ulteriori informazioni, consultare la sezione Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino. Tuttavia, se si desidera attivare i computer virtuali Virtual Standby a partire dal server Hyper-V, è possibile utilizzare la Gestione Hyper-V.

Nota: la Gestione Hyper-V consente di accedere alle snapshot del punto di ripristino create da CA ARCserve Central Virtual Standby per la protezione del nodo. Si consiglia di non eliminare le snapshot. Quando le snapshot vengono eliminate, le relazione esistente tra i dati contenuti nelle snapshot diventerà inconsistente alla successiva esecuzione di Virtual Standby. I dati inconsistenti non consentono la corretta attivazione dei computer Virtual Standby.

Per attivare i computer virtuali Virtual Standby dalla Gestione Hyper-V:

1. Accedere al server Hyper-V che esegue il monitoraggio dei nodi protetti.
2. Avviare la Gestione Hyper-V eseguendo una delle seguenti operazioni:

   Fare clic Start, Tutti i programmi, selezionare Strumenti di amministrazione e fare clic su Gestione Hyper-V.

   Viene visualizzata la Gestione Hyper-V.
3. Dalla struttura di directory di Gestione Hyper-V, espandere la Gestione Hyper-V e fare clic sul server Hyper-V contenente il computer virtuale che si desidera attivare.

   I computer virtuali al server Hyper-V specificato vengono visualizzati nell'elenco di computer virtuali del riquadro centrale.

4. Eseguire una delle seguenti operazioni:

   - **Per attivare il computer virtuale mediante la snapshot più recente:** dall'elenco Computer virtuali, fare clic con il tasto destro del mouse sul computer virtuale che si desidera attivare, quindi fare clic su Avvia del menu di scelta rapida.
   - **Per attivare il computer virtuale mediante una snapshot meno recente:**

     a. Dall'elenco Computer virtuali, selezionare il computer virtuale che si desidera attivare.

        Le snapshot associate al computer virtuale vengono visualizzate nell'elenco Snapshot.

     b. Fare clic con il tasto destro del mouse sulla snapshot che si desidera utilizzare per attivare il computer virtuale, quindi fare clic su Applica del menu di scelta rapida.

        Viene visualizzata la finestra di dialogo di applicazione della snapshot.

     c. Fare clic su Applica.

     d. Dall'elenco Computer virtuali, fare clic con il tasto destro del mouse sul computer virtuale che si desidera attivare, quindi fare clic su Avvia del menu di scelta rapida.

   Il computer virtuale Virtual Standby viene attivato.

Se necessario, è possibile eseguire il backup dei computer virtuali e creare snapshot del punto di ripristino dopo aver attivato il computer virtuale. Per ulteriori informazioni, consultare la sezione relativa alle attività da eseguire dopo l'attivazione di computer virtuali Virtual Standby.

Attivazione di computer virtuali Virtual Standby dal client VMware vSphere

Se si desidera attivare manualmente computer virtuali Virtual Standby, si consiglia di eseguire tale procedura dalla schermata Virtual Standby del server CA ARCserve D2D. Per ulteriori informazioni, consultare la sezione Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino. Tuttavia, se si desidera avviare i computer virtuali Virtual Standby a partire dal sistema server ESX o vCenter è possibile utilizzare il client VMware vSphere.

Nota: il client VMware vSphere consente di accedere alle snapshot del punto di ripristino create da CA ARCserve Central Virtual Standby per la protezione del nodo. Si consiglia di non eliminare le snapshot. Quando le snapshot vengono eliminate, le relazione esistente tra i dati contenuti nelle snapshot diventerà inconsistente alla successiva esecuzione di Virtual Standby. I dati inconsistenti non consentono la corretta attivazione dei computer Virtual Standby.

Per attivare computer virtuali Virtual Standby dal client VMware vSphere:

1. Aprire il client VMware vSphere ed accedere al sistema server ESX o vCenter che esegue il monitoraggio dei nodi protetti.

   Dalla struttura di directory, espandere il sistema server ESX o vCenter, individuare e selezionare il computer virtuale che si desidera attivare.

2. Eseguire una delle seguenti operazioni:

   - **Per attivare il computer virtuale mediante la snapshot più recente:** fare clic sulla scheda Introduzione, quindi selezionare l'opzione di attivazione del computer virtuale situata nella parte inferiore della schermata.
   - **Per attivare il computer virtuale mediante una snapshot meno recente:**

     a. Fare clic sul pulsante di gestione snapshot della barra degli strumenti.

        Viene visualizzata la finestra di dialogo Snapshot per (nome del computer virtuale) contenente un elenco delle snapshot disponibili per il computer virtuale.

     b. Selezionare la snapshot dall'elenco che si desidera utilizzare per l'attivazione del computer virtuale, quindi fare clic su Vai a.

   Il computer virtuale Virtual Standby viene attivato.

Se necessario, è possibile eseguire il backup dei computer virtuali e creare snapshot del punto di ripristino dopo aver attivato il computer virtuale. Per ulteriori informazioni, consultare la sezione relativa alle attività da eseguire dopo l'attivazione di computer virtuali Virtual Standby.

Protezione dei computer virtuali di Virtual Standby dopo l'attivazione

Dopo l'attivazione (manuale o automatica) di un computer virtuale Virtual Standby, il processo di backup di CA ARCserve D2D e il processo Virtual Standby non vengono eseguiti come pianificato. Se si desidera riprendere i processi dopo l'attivazione del computer virtuale di Virtual Standby, procedere nel seguente modo:

1. Modificare il prefisso del nome del computer virtuale nel criterio Virtual Standby.

   Al momento dell'attivazione dei computer virtuali Virtual Standby, l'applicazione definisce i nomi dei computer virtuale attivi come la concatenazione dell'opzione Prefisso nome del computer virtuale specificata nel criterio Virtual Standby e del nome host del nodo di origine.

Esempio:

- Prefisso del nome del computer virtuale: AA_
- Nome host del nodo di origine: Server1
- Nome del computer virtuale Virtual Standby: AA_Server1

Dopo l'attivazione dei computer virtuali, possono verificarsi conflitti di nome se non si modifica il prefisso del nome del computer virtuale nel criterio Virtual Standby. Problemi di questo tipo si verificano quando i nodi di origine e i computer virtuali Virtual Standby risiedono sullo stesso hypervisor.

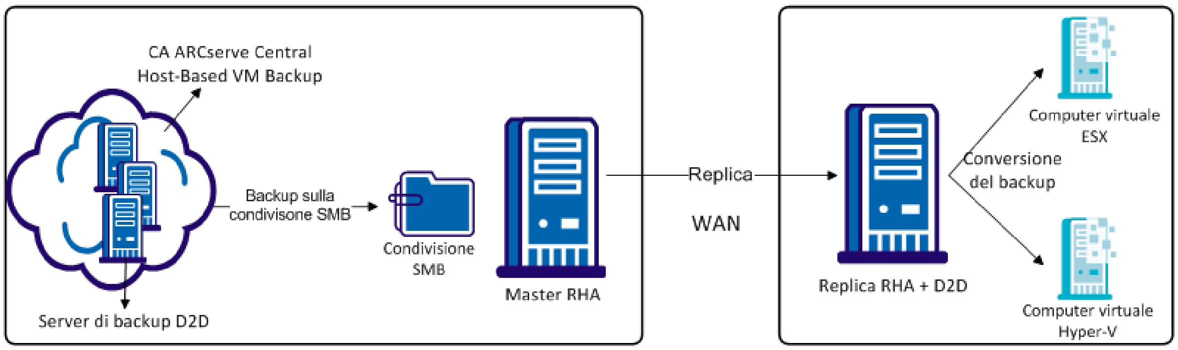
Per informazioni sulla modifica del prefisso del nome del computer virtuale nel criterio Virtual Standby, consultare la sezione Modifica dei criteri (a pagina 76). Se necessario, è possibile aggiornare altre impostazioni del criterio Virtual Standby. In alternativa, è possibile creare un nuovo criterio per proteggere il computer virtuale Virtual Standby. Per informazioni sulla creazione di nuovi criteri, consultare la sezione Creazione dei criteri CA ARCserve Central Virtual Standby (a pagina 40).

2. Dopo aver aggiornato il criterio o creato un nuovo criterio, effettuare la distribuzione del criterio sul computer virtuale Virtual Standby. Per ulteriori informazioni, consultare la sezione Distribuzione dei criteri (a pagina 55).
3. Dopo aver effettuato la distribuzione del criterio sul computer virtuale Virtual Standby, riprendere il processo Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby.
4. Dopo aver effettuato la distribuzione del criterio, accedere a CA ARCserve D2D sul computer virtuale Virtual Standby e pianificare un metodo di ripetizione per il processo di backup di CA ARCserve D2D. Per ulteriori informazioni, consultare la *Guida per l'utente di CA ARCserve D2D*.

Nota: CA ARCserve Central Protection Manager e CA ARCserve Central Virtual Standby dispongono di un meccanismo che consente di eseguire la risincronizzazione automatica dei criteri con i nodi gestiti di CA ARCserve D2D su base settimanale. Questo meccanismo consente a CA ARCserve Central Protection Manager di riavviare i processi di backup sui computer virtuali Virtual Standby ridistribuendo il criterio in atto sul nodo di CA ARCserve D2D sul computer virtuale Virtual Standby. Il processo di distribuzione criterio si comporta in tal modo poiché il nodo di origine e il computer virtuale Virtual Standby hanno lo stesso nome host, che consente a CA ARCserve Central Protection Manager di risincronizzare il criterio. L'unico limite a questo comportamento è dato dal fatto che il server CA ARCserve Central Protection Manager e il computer virtuale Virtual Standby devono essere in grado di comunicare tra loro in rete. Una volta completata la risincronizzazione e la distribuzione del criterio sul computer virtuale Virtual Standby, riprendere il processo Virtual Standby sul computer virtuale. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby.

Attivazione dei computer virtuali remoti di Virtual Standby

Questo scenario descrive le procedure usate dai manager dell'archiviazione per utilizzare e integrare le funzionalità già disponibili in CA ARCserve Replication per lo spostamento dei punti di ripristino di CA ARCserve D2D e CA ARCserve Central Host-Based VM Backup su posizioni esterne. Questa funzionalità consente a CA ARCserve Central Virtual Standby di convertire tali punti di ripristino replicati e registrarli automaticamente con Microsoft Hyper-V, VMWare vCenter o ESXi.



La tabella seguente riporta le sezioni che descrivono le attività di attivazione dei computer di standby virtuale:

Attività	**Sezione**
Attivazione di computer virtuali remoti di standby virtuale dalle snapshot del punto di ripristino replicato in caso di errore del server di origine.	Attivazione di computer virtuali remoti di standby virtuale a partire da snapshot dei punti di ripristino (a pagina 118)
Protezione dei computer virtuali di standby virtuale dopo l'attivazione dei computer virtuali.	Protezione dei computer virtuali di Virtual Standby dopo l'attivazione (a pagina 123)

Attivazione di computer virtuali Virtual Standby a partire da snapshot dei punti di ripristino

È possibile configurare Virtual Standby per attivare i computer virtuali remoti di Virtual Standby dalle istantanee dei punti di ripristino replicati in caso di errore del server di origine, di una condizione di emergenza o per la manutenzione non in linea di un nodo di origine.

Nota: le operazioni riportate di seguito descrivono la procedura di attivazione dei computer virtuali di Virtual Standby dalle snapshot dei punti di ripristino replicati.

Procedere come descritto di seguito:

1. Nella barra di navigazione, fare clic su Virtual Standby, quindi su Nodi per visualizzare la schermata corrispondente.
2. Dall'elenco Gruppi, fare clic su Tutti i nodi oppure sul gruppo contenente il nodo CA ARCserve D2D o CA ARCserve Central Host-Based VM Backup a cui si desidera accedere.

   Nell'elenco dei nodi verranno visualizzati tutti i nodi associati al gruppo specificato.
3. Individuare e selezionare il nodo contenente i computer virtuali di standby creati da un punto di ripristino replicato da attivare. Fare clic su una delle seguenti opzioni del menu di scelta rapida:
   - **Configurazione di rete del computer virtuale di standby**
     - Specificare la rete virtuale, la scheda di interfaccia di rete (NIC) e le impostazioni TCP/IP per ciascuna scheda di rete nella scheda Impostazioni della scheda di rete.

     OPPURE
     - Aggiornare i server DNS per reindirizzare i client dal computer di origine ai computer virtuali di standby virtuale in base alle impostazioni TCP/IP della scheda Impostazioni di aggiornamento DNS.
   - **Computer virtuale di standby:**
     - Selezionare un intervallo di tempo della snapshot del punto di ripristino per l'attivazione del computer virtuale.

     OPPURE
     - Selezionare la casella di controllo Attivare il computer di standby virtuale con configurazioni di rete personalizzate per aprire la finestra di dialogo Configurazione di rete del computer virtuale di standby.

       Nota: se il computer virtuale di standby non è ancora stato configurato, verrà visualizzato il collegamento: La rete del computer virtuale di standby non è configurata. Fare clic su questo collegamento per configurare la rete.

   Fare clic su Salva.

Le impostazioni vengono salvate per il computer virtuale remoto di standby virtuale.

Nota: dopo l'attivazione del computer virtuale è possibile che venga chiesto di riavviare il computer una o più volte. Ciò si verifica se VMware installa gli strumenti VMware o Windows Hyper-V installa i servizi di integrazione sul computer virtuale.

Una volta attivati i computer virtuali remoti di Virtual Standby dalle snapshot del punto di ripristino, potrebbe essere necessario effettuare le seguenti attività:

- Attivare il sistema operativo di Windows in esecuzione sul computer virtuale.
- Avviare i backup di CA ARCserve D2D sul computer virtuale.

  Nota: per informazioni sulla creazione e l'assegnazione di criteri di backup di CA ARCserve D2D mediante CA ARCserve Central Protection Manager, consultare la *Guida per l'utente di CA ARCserve Central Protection Manager.*

- Aggiornare CA ARCserve Central Virtual Standby con il nome host, l'indirizzo IP, e le credenziali di accesso per il computer virtuale.
- Assegnare il nodo a un criterio.

  Nota: questa attività è richiesta solo se si desidera creare snapshot del punto di ripristino per il computer virtuale attivo. Per ulteriori informazioni, consultare la sezione Assegnazione dei nodi a un criterio (a pagina 53).

Attivazione di computer virtuali di Virtual Standby dalla Gestione Hyper-V

Se si desidera attivare i computer virtuali remoti di Virtual Standby a partire dal server Hyper-V, è possibile utilizzare la Gestione Hyper-V.

Nota: la Gestione Hyper-V consente di accedere alle snapshot del punto di ripristino replicato da CA ARCserve Replication and High Availability e convertite da CA ARCserve Central Virtual Standby per la protezione del nodo. Si consiglia di non eliminare le snapshot. Quando le snapshot vengono eliminate, le relazione esistente tra i dati contenuti nelle snapshot diventerà inconsistente alla successiva esecuzione di Virtual Standby. I dati inconsistenti non consentono la corretta attivazione dei computer Virtual Standby.

Procedere come descritto di seguito:

1. Accedere al server Hyper-V che esegue il monitoraggio dei nodi protetti.
2. Avviare la Gestione Hyper-V eseguendo una delle seguenti operazioni:

   Per aprire la Gestione Hyper-V , fare clic su Start, Tutti i Programmi, Strumenti di amministrazione, e selezionare Gestione Hyper-V Gestione.

3. Dalla struttura di directory della Gestione Hyper-V, espandere la Gestione Hyper-V e fare clic sul server Hyper-V contenente il computer virtuale che si desidera attivare.

   I computer virtuali al server Hyper-V specificato vengono visualizzati nell'elenco di computer virtuali del riquadro centrale.

4. Eseguire una delle seguenti operazioni:

   - **Per attivare il computer virtuale remoto utilizzando la snapshot più recente:** dall'elenco Computer virtuali, fare clic con il tasto destro del mouse sul computer virtuale che si desidera attivare, quindi fare clic su Avvia del menu di scelta rapida.
   - **Per attivare il computer virtuale utilizzando una snapshot precedente:**

     a. Dall'elenco Computer virtuali, selezionare il computer virtuale che si desidera attivare.

        Le snapshot associate al computer virtuale vengono visualizzate nell'elenco Snapshot.

     b. Fare clic con il tasto destro del mouse sulla snapshot che si desidera utilizzare per attivare il computer virtuale remoto, quindi fare clic su Applica del menu di scelta rapida per aprire la finestra di dialogo di applicazione della snapshot.

     c. Fare clic su Applica.

     d. Dall'elenco Computer virtuali, fare clic con il tasto destro del mouse sul computer virtuale che si desidera attivare, quindi fare clic su Avvia del menu di scelta rapida.

   Il computer virtuale remoto di Virtual Standby viene attivato.

Se necessario, è possibile eseguire il backup dei computer virtuali remoti e creare snapshot del punto di ripristino dopo aver attivato il computer virtuale. Per ulteriori informazioni, consultare la sezione relativa alle attività da eseguire dopo l'attivazione di computer virtuali Virtual Standby.

Attivazione di computer virtuali remoti di Virtual Standby dal client VMware vSphere

Se si desidera avviare i computer virtuali remoti di Virtual Standby a partire dal sistema server ESX o vCenter è possibile utilizzare il client VMware vSphere.

Nota: la il client VMware vSphere consente di accedere alle snapshot del punto di ripristino replicato da CA ARCserve Replication and High Availability e convertito da CA ARCserve Central Virtual Standby per la protezione del nodo. Si consiglia di non eliminare le snapshot. Quando le snapshot vengono eliminate, le relazione esistente tra i dati contenuti nelle snapshot diventerà inconsistente alla successiva esecuzione di Virtual Standby. I dati inconsistenti non consentono la corretta attivazione dei computer Virtual Standby.

Procedere come descritto di seguito:

1. Aprire il client VMware vSphere ed accedere al sistema server ESX o vCenter che esegue il monitoraggio dei nodi protetti.

   Dalla struttura di directory, espandere il sistema server ESX o vCenter, individuare e selezionare il computer virtuale che si desidera attivare.

2. Eseguire una delle seguenti operazioni:

   - **Per attivare il computer virtuale remoto utilizzando la snapshot più recente:** fare clic sulla scheda Introduzione, quindi selezionare l'opzione Attiva computer virtuale disponibile nella parte inferiore della schermata.

   - **Per attivare il computer virtuale utilizzando una snapshot precedente:**

     a. Dal client VMware vSphere, fare clic con il pulsante destro del mouse sul nome del computer virtuale di cui si desidera acquisire snapshot, quindi selezionare il pulsante di gestione shapshot. Verrà visualizzata la finestra di dialogo Snapshot per <nome del computer virtuale> contenente un elenco delle snapshot disponibili per il computer virtuale remoto.

     b. Selezionare la snapshot che si desidera utilizzare per l'attivazione del computer virtuale remoto, quindi fare clic su Vai a.

   Il computer virtuale remoto di Virtual Standby viene attivato.

Se necessario, è possibile eseguire il backup dei computer virtuali e creare snapshot del punto di ripristino dopo aver attivato il computer virtuale. Per ulteriori informazioni, consultare la sezione relativa alle attività da eseguire dopo l'attivazione di computer virtuali Virtual Standby.

Protezione dei computer virtuali remoti di Virtual Standby dopo l'attivazione

Dopo l'attivazione di un computer virtuale remoto di Virtual Standby, il processo di backup di CA ARCserve D2D e il processo Virtual Standby non vengono eseguiti come pianificato. Se si desidera riprendere i processi dopo l'attivazione del computer virtuale remoto di Virtual Standby, procedere come segue:

1. Modificare il prefisso del nome del computer virtuale nel criterio Virtual Standby.

   Al momento dell'attivazione dei computer virtuali remoti di Virtual Standby da parte di CA ARCserve Central Virtual Standby, l'applicazione definisce i nomi dei computer virtuale remoti attivi concatenando l'opzione Prefisso nome del computer virtuale specificata nel criterio Virtual Standby e il nome host del nodo di origine.

   Esempio:

   - Prefisso del nome del computer virtuale: AA_
   - Nome host del nodo di origine: Server1
   - Nome del computer virtuale Virtual Standby: AA_Server1

   Dopo l'attivazione dei computer virtuali remoti di Virtual Standby, potrebbero verificarsi conflitti di nome se non si modifica il prefisso del nome del computer virtuale nel criterio Virtual Standby. Problemi di questo tipo si verificano quando i nodi di origine e i computer virtuali remoti di Virtual Standby risiedono sullo stesso hypervisor.

   Per informazioni sulla modifica del prefisso del nome del computer virtuale nel criterio Virtual Standby, consultare la sezione Modifica dei criteri. Se necessario, è possibile aggiornare altre impostazioni del criterio Virtual Standby. Se lo si desidera, è possibile creare un nuovo criterio Virtual Standby per proteggere il computer virtuale remoto di Virtual Standby. Per informazioni sulla creazione di nuovi criteri, consultare la sezione Creazione dei criteri CA ARCserve Central Virtual Standby (a pagina 40).

2. Dopo aver aggiornato il criterio o aver creato un nuovo criterio, effettuare la distribuzione del criterio sul computer virtuale remoto di Virtual Standby. Per ulteriori informazioni, consultare la sezione Distribuzione dei criteri (a pagina 55).

3. Dopo aver effettuato la distribuzione del criterio sul computer virtuale remoto di Virtual Standby, riprendere il processo Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby (a pagina 103).

4. Dopo aver effettuato la distribuzione del criterio, accedere a CA ARCserve D2D sul computer virtuale remoto di Virtual Standby e pianificare un metodo di ripetizione per il processo di backup di CA ARCserve D2D. Per ulteriori informazioni, consultare la *Guida per l'utente di CA ARCserve D2D*.

Nota: CA ARCserve Central Protection Manager e CA ARCserve Central Virtual Standby dispongono di un meccanismo che consente di eseguire la risincronizzazione automatica dei criteri con i nodi gestiti di CA ARCserve D2D su base settimanale. Questo meccanismo consente a CA ARCserve Central Protection Manager di riavviare i processi di backup sui computer virtuali remoti di Virtual Standby ridistribuendo il criterio del nodo di CA ARCserve D2D sul computer virtuale remoto di Virtual Standby. Il processo di distribuzione del criterio si comporta in tal modo perché il nodo di origine e il computer virtuale remoto di Virtual Standby presentano lo stesso nome host, consentendo a CA ARCserve Central Protection Manager di risincronizzare il criterio. L'unico limite a questo comportamento è dato dal fatto che il server CA ARCserve Central Protection Manager e il computer virtuale remoto di Virtual Standby devono essere in grado di comunicare in rete. Una volta completata la risincronizzazione e la distribuzione del criterio sul computer virtuale remoto di Virtual Standby, riprendere il processo di Virtual Standby sul computer virtuale remoto di Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby (a pagina 103).

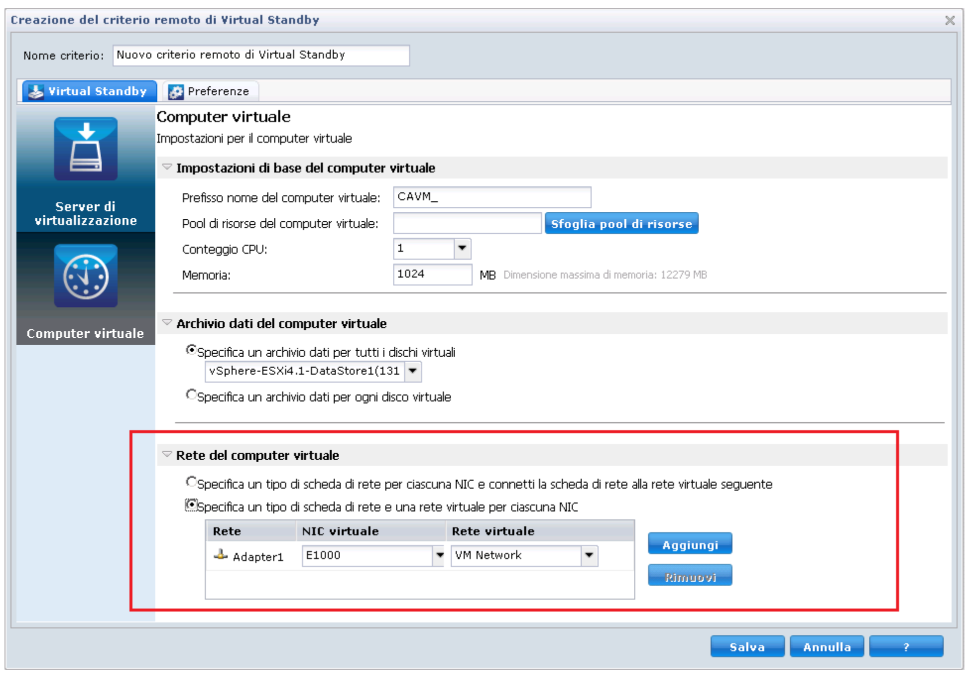
Definizione del numero di NIC da attivare

Durante l'attivazione dei computer virtuali, Virtual Standby determina il numero di schede di interfaccia di rete da attivare in base alla configurazione della rete del computer virtuale di standby. La tabella seguente descrive la modalità utilizzata da Virtual Standby per determinare il numero di schede di interfaccia di rete da attivare al momento dell'attivazione dei computer virtuali di standby:

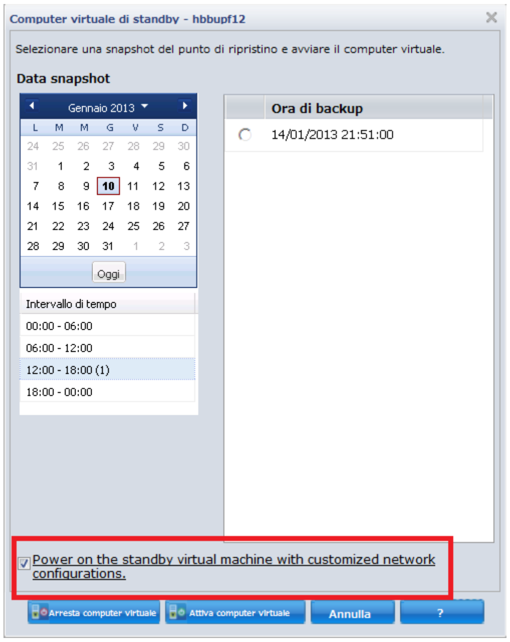
Valori definiti nel criterio di rete del computer virtuale	**L'opzione Attivare il computer di standby virtuale con configurazioni di rete personalizzate *non viene* specificata.**	**L'opzione Attivare il computer di standby virtuale con configurazioni di rete personalizzate *viene* specificata.**
I valori definiti sono identici ai valori del computer di origine.	Virtual Standby attiva il numero di NIC definito per il computer di origine a partire dall'ultimo processo di backup.	La quantità di NIC attivate da Virtual Standby si basa sul valore più elevato tra i seguenti valori: ■ Il numero definito nella configurazione di rete personalizzata. ■ Il numero di NIC definito per il computer di origine a partire dall'ultimo processo di backup.

Valori definiti nel criterio di rete del computer virtuale	L'opzione Attivare il computer di standby virtuale con configurazioni di rete personalizzate *non viene* specificata.	L'opzione Attivare il computer di standby virtuale con configurazioni di rete personalizzate *viene* specificata.
I valori definiti sono valori personalizzati.	Virtual Standby attiva il numero di reti personalizzate definite nel criterio.	La quantità di NIC attivate da Virtual Standby si basa sul valore più elevato tra i seguenti valori: ■ Il numero definito nella configurazione di rete personalizzata. ■ Il numero di NIC definito per il criterio personalizzato.

La finestra di dialogo seguente (Modifica del criterio locale di Virtual Standby) mostra la posizione in cui vengono definiti i criteri costituiti dalle configurazioni personalizzate delle NIC da attivare:



La finestra di dialogo seguente (Computer virtuale di standby - <host_name>) mostra la posizione in cui viene specificata l'opzione di accensione del computer virtuale.



Protezione dei computer virtuali Virtual Standby attivati

Dopo l'attivazione (manuale o automatica) di un computer virtuale Virtual Standby, il processo di backup di CA ARCserve D2D e il processo Virtual Standby non vengono eseguiti come pianificato. Se si desidera riprendere i processi dopo l'attivazione del computer virtuale di Virtual Standby, procedere nel seguente modo:

1. Modificare il prefisso del nome del computer virtuale nel criterio Virtual Standby.

   Al momento dell'attivazione dei computer virtuali Virtual Standby, l'applicazione definisce i nomi dei computer virtuale attivi come la concatenazione dell'opzione Prefisso nome del computer virtuale specificata nel criterio Virtual Standby e del nome host del nodo di origine.

Esempio:

- Prefisso del nome del computer virtuale: AA_
- Nome host del nodo di origine: Server1
- Nome del computer virtuale Virtual Standby: AA_Server1

Dopo l'attivazione dei computer virtuali, possono verificarsi conflitti di nome se non si modifica il prefisso del nome del computer virtuale nel criterio Virtual Standby. Problemi di questo tipo si verificano quando i nodi di origine e i computer virtuali Virtual Standby risiedono sullo stesso hypervisor.

Per informazioni sulla modifica del prefisso del nome del computer virtuale nel criterio Virtual Standby, consultare la sezione Modifica dei criteri (a pagina 76). Se necessario, è possibile aggiornare altre impostazioni del criterio Virtual Standby. In alternativa, è possibile creare un nuovo criterio per proteggere il computer virtuale Virtual Standby. Per informazioni sulla creazione di nuovi criteri, consultare la sezione Creazione dei criteri CA ARCserve Central Virtual Standby (a pagina 40).

2. Dopo aver aggiornato il criterio o creato un nuovo criterio, effettuare la distribuzione del criterio sul computer virtuale Virtual Standby. Per ulteriori informazioni, consultare la sezione Distribuzione dei criteri (a pagina 55).
3. Dopo aver effettuato la distribuzione del criterio sul computer virtuale Virtual Standby, riprendere il processo Virtual Standby. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby.
4. Dopo aver effettuato la distribuzione del criterio, accedere a CA ARCserve D2D sul computer virtuale Virtual Standby e pianificare un metodo di ripetizione per il processo di backup di CA ARCserve D2D. Per ulteriori informazioni, consultare la *Guida per l'utente di CA ARCserve D2D*.

Nota: CA ARCserve Central Protection Manager e CA ARCserve Central Virtual Standby dispongono di un meccanismo che consente di eseguire la risincronizzazione automatica dei criteri con i nodi gestiti di CA ARCserve D2D su base settimanale. Questo meccanismo consente a CA ARCserve Central Protection Manager di riavviare i processi di backup sui computer virtuali Virtual Standby ridistribuendo il criterio in atto sul nodo di CA ARCserve D2D sul computer virtuale Virtual Standby. Il processo di distribuzione criterio si comporta in tal modo poiché il nodo di origine e il computer virtuale Virtual Standby hanno lo stesso nome host, che consente a CA ARCserve Central Protection Manager di risincronizzare il criterio. L'unico limite a questo comportamento è dato dal fatto che il server CA ARCserve Central Protection Manager e il computer virtuale Virtual Standby devono essere in grado di comunicare tra loro in rete. Una volta completata la risincronizzazione e la distribuzione del criterio sul computer virtuale Virtual Standby, riprendere il processo Virtual Standby sul computer virtuale. Per ulteriori informazioni, consultare la sezione Sospensione e riattivazione dei processi Virtual Standby.

Capitolo 7: Ripristino dei dati

Questa sezione contiene i seguenti argomenti:

Ripristino dei dati dai punti di ripristino di CA ARCserve D2D

Virtual Standby consente di recuperare i dati dai punti di ripristino disponibili. I punti di ripristino sono snapshot temporizzate di dati presenti sui nodi di origine di CA ARCserve D2D. Dai punti di ripristino è possibile specificare il dati che si desidera recuperare.

Per ripristinare i dati dai punti di ripristino di CA ARCserve D2D

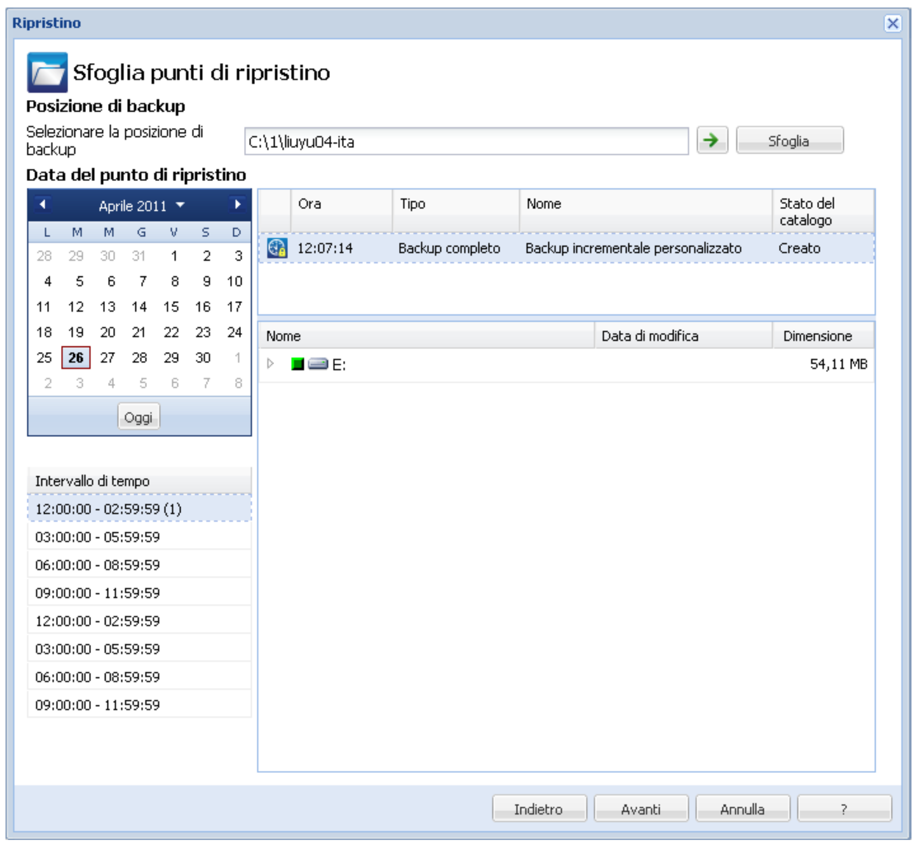
1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Nella finestra di dialogo Ripristino, fare clic su Sfoglia punti di ripristino.

   Verrà visualizzata la finestra di dialogo Sfoglia punti di ripristino.



3. Specificare l'origine di backup. È possibile specificare una posizione oppure individuare il percorso di archiviazione delle immagini di backup. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso. Fare clic sull'icona di convalida con la freccia verde per verificare che l'accesso alla posizione di origine sia stato eseguito correttamente.

   La visualizzazione calendario evidenzierà (in verde) tutte le date relative al periodo di tempo contenente i punti di ripristino per l'origine di backup selezionata.

4. Specificare i dati di cui si desidera eseguire il ripristino.

   a. Nel calendario, selezionare la data dell'immagine di backup da ripristinare.

      Verranno visualizzati, quindi, i punti di ripristino associati alla data, unitamente all'ora di backup, al tipo di backup eseguito e al nome del backup.

   b. Selezionare un punto di ripristino.

      Verrà visualizzato il contenuto del backup (eventuali applicazioni incluse) per il punto di ripristino selezionato.

      Nota: l'icona di un orologio con lucchetto indica che il punto di ripristino contiene informazioni crittografate e potrebbe richiedere una password per il ripristino.

   c. Selezionare il contenuto da ripristinare.

      ■ Per un ripristino a livello di volume, è possibile scegliere di ripristinare l'intero volume oppure alcuni file/cartelle specifici.

      ■ Per un ripristino a livello di applicazione, è possibile scegliere di ripristinare l'intera applicazione o solo determinati componenti, database, istanze, ecc. dell'applicazione.

5. Dopo aver specificato i dati di cui si desidera eseguire il ripristino, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

6. Selezionare le seguenti opzioni nella finestra di dialogo Opzioni di ripristino:

   ■ **Destinazione** - Selezionare la destinazione di ripristino.

      – Ripristina in posizione originale - È possibile ripristinare i dati nella posizione di origine utilizzata per l'acquisizione dell'immagine di backup.

      – Ripristina su - È possibile specificare una posizione o individuare il percorso verrà eseguito il ripristino delle immagini di backup. Fare clic sulla freccia accanto al campo Ripristina per verificare la connessione alla posizione specificata.

        Potrebbe essere necessario immettere le credenziali Nome utente e Password per potere accedere al percorso.

- **Risolvere Conflitti** - Specifica la modalità utilizzata da CA ARCserve D2D per la risoluzione dei conflitti rilevati durante il processo di ripristino.
  - Sovrascrivi i file esistenti - Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dal file di backup, indipendentemente dalla loro presenza sul computer.
  - Sostituisci file attivi - Sostituisce i file attivi al riavvio. Se durante il tentativo di ripristino CA ARCserve D2D rileva che il file esistente è in uso, tale file non verrà sostituito immediatamente. Per evitare eventuali problemi, i file attivi verranno sostituiti al successivo riavvio del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita al riavvio successivo).

    Nota: se l'opzione non è selezionata, i file attivi non verranno inclusi nel ripristino.
  - Rinomina file - Crea un nuovo file se il nome file è già esistente. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno ripristinati sul nuovo file.
  - Ignora file esistenti - Consente di ignorare e non sovrascrivere i file esistenti contenuti nella destinazione di ripristino. Verrà eseguito soltanto il ripristino dai file di backup degli oggetti non presenti sul computer.

    Questa opzione è selezionata per impostazione predefinita.

- **Struttura directory** - Specifica le operazioni che CA ARCserve D2D potrà eseguire nella struttura della directory durante il processo di ripristino.
  - Crea directory principale - Se l'immagine di backup acquisita contiene una struttura di directory principale, CA ARCserve D2D ricreerà la stessa struttura di directory nel percorso di destinazione di ripristino.

    Se l'opzione Crea directory principale non è selezionata, il file o la cartella da ripristinare verranno ripristinati direttamente nella cartella di destinazione.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

    Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e "D:\Restore\B.txt. La directory principale al di sopra del livello di file specificato non verrà ricreata.

    Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

    Se l'opzione Crea directory principale è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt, e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

    Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).

    Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

- **Password di Crittografia** - Se i dati del punto di ripristino selezionato sono crittografati, potrebbe essere necessario specificare la password di crittografia.

  Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup crittografato, la password non verrà richiesta. La password verrà richiesta se viene eseguito il ripristino su un computer diverso.

  Nota: le icone riportate di seguito indicano se il punto di ripristino contiene informazioni crittografate e se è richiesta l'immissione di una password per il ripristino.

  Punto di ripristino non crittografato:

  Punto di ripristino crittografato:

Fare clic su Avanti.

Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

7. Verificare che le informazioni della finestra di dialogo Riepilogo di Ripristino siano corrette.

   Nota: se si desidera modificare le opzioni di ripristino specificate, fare clic su Indietro per tornare alla finestra di dialogo corrispondente.

   Fare clic su Fine.

Le opzioni di ripristino verranno applicate e verrà eseguito il recupero dei dati.

Ripristino di dati dalle copie di file di CA ARCserve D2D

Virtual Standby consente di eseguire il ripristino di dati da copie di file di CA ARCserve D2D. Le copie di file sono copie dei punti di ripristino di CA ARCserve D2D eseguite su supporti di archiviazione non in linea, quali dischi o cloud. Dalle copie di file è possibile specificare i dati che si desidera recuperare.

Per ripristinare i dati dalle copie di file di CA ARCserve D2D

1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

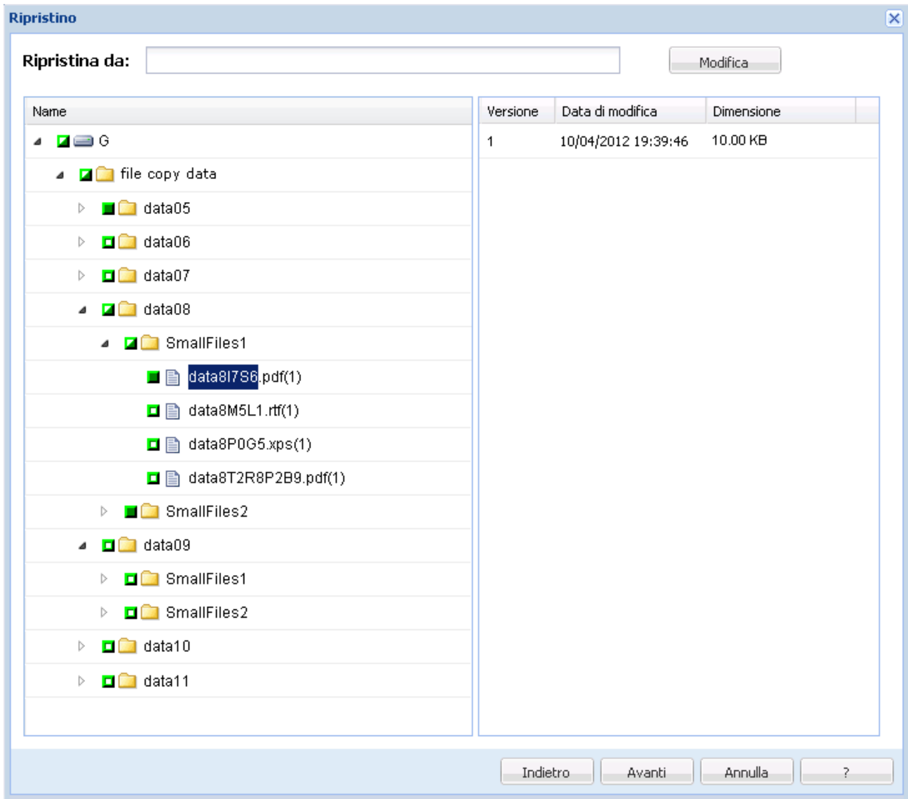
   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Dalla finestra di dialogo Ripristino, fare clic su Sfoglia copie file.

   Verrà visualizzata la finestra di dialogo Sfoglia copie file, come illustrato nella seguente schermata:

   Nota: la destinazione visualizzata nel riquadro a destra corrisponde alla destinazione predefinita.

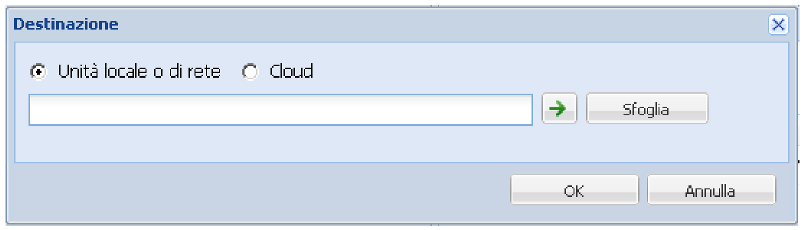


3. Nel riquadro Nome, specificare il dati di copia file che si desidera recuperare. È possibile specificare il volume oppure una combinazione qualsiasi di file e cartelle.

   Se si seleziona il ripristino di un solo file, nel riquadro a destra verranno visualizzate tutte le versioni copiate per tale file. Se sono disponibili più versioni, selezionare la versione di copia file desiderata.

   - **Modifica destinazione** - Consente di selezionare una posizione di archiviazione alternativa per le immagini di copia di file.

     Verrà visualizzata una finestra di dialogo contenente le opzioni di destinazione alternative disponibili.



   - **Unità locale o di rete** - Verrà visualizzata la finestra di dialogo di selezione della posizione di backup, che consente di individuare e selezionare una posizione alternativa su unità locali o di rete.
   - **Cloud** - Verrà visualizzata la finestra di dialogo Configurazione cloud, che consente di accedere e configurare una posizione cloud alternativa.

4. Fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

5. Selezionare le seguenti opzioni nella finestra di dialogo Opzioni di ripristino:

   - **Destinazione** - Selezionare la destinazione di ripristino.
     - Ripristina in posizione originale - È possibile ripristinare i dati nella posizione di origine utilizzata per l'acquisizione dell'immagine di backup.
     - Ripristina su - È possibile specificare una posizione o individuare il percorso verrà eseguito il ripristino delle immagini di backup. Fare clic sulla freccia accanto al campo Ripristina per verificare la connessione alla posizione specificata.

       Potrebbe essere necessario immettere le credenziali Nome utente e Password per potere accedere al percorso.

- **Risolvere Conflitti** - Specifica la modalità utilizzata da CA ARCserve D2D per la risoluzione dei conflitti rilevati durante il processo di ripristino.
  - Sovrascrivi i file esistenti - Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dal file di backup, indipendentemente dalla loro presenza sul computer.
  - Sostituisci file attivi - Sostituisce i file attivi al riavvio. Se durante il tentativo di ripristino CA ARCserve D2D rileva che il file esistente è in uso, tale file non verrà sostituito immediatamente. Per evitare eventuali problemi, i file attivi verranno sostituiti al successivo riavvio del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita al riavvio successivo).

    Nota: se l'opzione non è selezionata, i file attivi non verranno inclusi nel ripristino.
  - Rinomina file - Crea un nuovo file se il nome file è già esistente. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno ripristinati sul nuovo file.
  - Ignora file esistenti - Consente di ignorare e non sovrascrivere i file esistenti contenuti nella destinazione di ripristino. Verrà eseguito soltanto il ripristino dai file di backup degli oggetti non presenti sul computer.

    Questa opzione è selezionata per impostazione predefinita.

- **Struttura directory** - Specifica le operazioni che CA ARCserve D2D potrà eseguire nella struttura della directory durante il processo di ripristino.
  - Crea directory principale - Se l'immagine di backup acquisita contiene una struttura di directory principale, CA ARCserve D2D ricreerà la stessa struttura di directory nel percorso di destinazione di ripristino.

    Se l'opzione Crea directory principale non è selezionata, il file o la cartella da ripristinare verranno ripristinati direttamente nella cartella di destinazione.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

    Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e "D:\Restore\B.txt. La directory principale al di sopra del livello di file specificato non verrà ricreata.

    Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

    Se l'opzione Crea directory principale è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt, e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

    Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).

    Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

- **Password di Crittografia** - Se i dati del punto di ripristino selezionato sono crittografati, potrebbe essere necessario specificare la password di crittografia.

  Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup crittografato, la password non verrà richiesta. La password verrà richiesta se viene eseguito il ripristino su un computer diverso.

  Nota: le icone riportate di seguito indicano se il punto di ripristino contiene informazioni crittografate e se è richiesta l'immissione di una password per il ripristino.

  Punto di ripristino non crittografato:

  Punto di ripristino crittografato:

Fare clic su Avanti.

Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

6. Verificare che le informazioni della finestra di dialogo Riepilogo di Ripristino siano corrette.

   Nota: se si desidera modificare le opzioni di ripristino specificate, fare clic su Indietro per tornare alla finestra di dialogo corrispondente.

   Fare clic su Fine.

Le opzioni di ripristino verranno applicate e verrà eseguito il recupero dei dati.

Ripristino di dati mediante l'opzione Trova file/cartelle da ripristinare

Virtual Standby consente di eseguire ricerche dei punti di ripristino e di copie di file di CA ARCserve D2D per il ripristino di file o cartelle specifici.

Per ripristinare i dati mediante l'opzione Trova file/cartelle da ripristinare

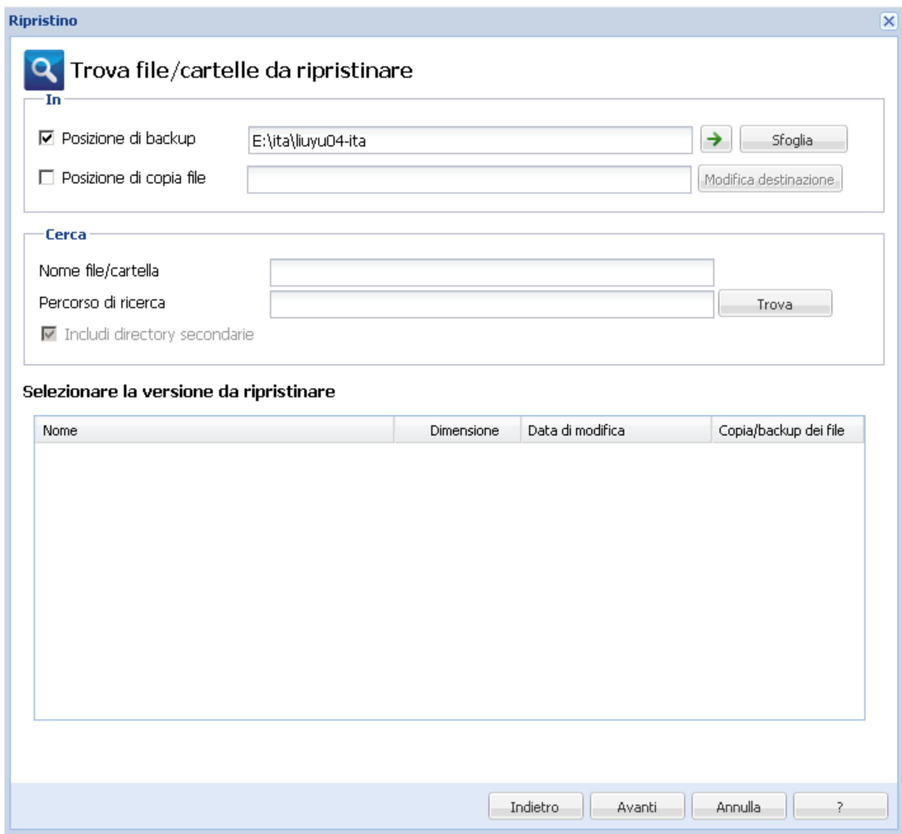
1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Dalla finestra di dialogo Ripristino, fare clic su Trova file/cartelle da ripristinare.

   Verrà visualizzata la finestra di dialogo Trova file/cartelle da ripristinare.



3. Specificare il percorso in cui eseguire la ricerca (origine di backup e/o archiviazione).

   È possibile specificare un percorso o individuare una posizione in cui sono memorizzare le immagini di backup/archiviazione. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso. Fare clic sull'icona di convalida con la freccia verde per verificare che l'accesso alla posizione di origine sia stato eseguito correttamente.

4. Specificare gli elementi da cercare (nome del file o della cartella da ripristinare).

   Nota: il campo Nome file supporta la ricerca per nome completo e con caratteri jolly. Se non si conosce il nome file completo, è possibile semplificare i risultati della ricerca immettendo i caratteri jolly "*" e "?" nel campo Nome file.

   I caratteri jolly supportati per il nome dei file o delle cartelle sono i seguenti:

   - * - Utilizzare l'asterisco per sostituire zero o più caratteri nel nome di un file o di una directory.
   - ? - utilizzare il punto interrogativo per sostituire un singolo carattere nel nome di un file o di una cartella.

   Ad esempio, specificando *.txt, la ricerca restituirà tutti i file con estensione .txt.

   Nota: se necessario, è possibile immettere un percorso per filtrare ulteriormente la ricerca e specificare se includere o meno le sottodirectory.

5. Fare clic su Trova per dare inizio alla ricerca.

   Verranno visualizzati i risultati di ricerca. Se la ricerca individua più occorrenze (punti di ripristino) dello stesso file di ricerca, verranno elencate tutte le occorrenze in ordine cronologico (dalla più recente alla meno recente). Verrà, inoltre, indicato se il file trovato è stato sottoposto a backup o archiviazione.

6. Selezionare la versione (occorrenza) del file o della cartella da ripristinare e fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Opzioni di ripristino.

7. Selezionare le seguenti opzioni nella finestra di dialogo Opzioni di ripristino:

   - **Destinazione** - Selezionare la destinazione di ripristino.
     - Ripristina in posizione originale - È possibile ripristinare i dati nella posizione di origine utilizzata per l'acquisizione dell'immagine di backup.
     - Ripristina su - È possibile specificare una posizione o individuare il percorso verrà eseguito il ripristino delle immagini di backup. Fare clic sulla freccia accanto al campo Ripristina per verificare la connessione alla posizione specificata.

       Potrebbe essere necessario immettere le credenziali Nome utente e Password per potere accedere al percorso.

- **Risolvere Conflitti** - Specifica la modalità utilizzata da CA ARCserve D2D per la risoluzione dei conflitti rilevati durante il processo di ripristino.
  - Sovrascrivi i file esistenti - Sovrascrive (sostituisce) i file esistenti nella destinazione di ripristino. Tutti gli oggetti verranno ripristinati dal file di backup, indipendentemente dalla loro presenza sul computer.
  - Sostituisci file attivi - Sostituisce i file attivi al riavvio. Se durante il tentativo di ripristino CA ARCserve D2D rileva che il file esistente è in uso, tale file non verrà sostituito immediatamente. Per evitare eventuali problemi, i file attivi verranno sostituiti al successivo riavvio del computer. (Il ripristino verrà eseguito immediatamente, ma la sostituzione dei file attivi verrà eseguita al riavvio successivo).

    Nota: se l'opzione non è selezionata, i file attivi non verranno inclusi nel ripristino.
  - Rinomina file - Crea un nuovo file se il nome file è già esistente. Consente di copiare il file di origine nella destinazione con lo stesso nome file ma con un'estensione diversa. I dati verranno ripristinati sul nuovo file.
  - Ignora file esistenti - Consente di ignorare e non sovrascrivere i file esistenti contenuti nella destinazione di ripristino. Verrà eseguito soltanto il ripristino dai file di backup degli oggetti non presenti sul computer.

    Questa opzione è selezionata per impostazione predefinita.

- **Struttura directory** - Specifica le operazioni che CA ARCserve D2D potrà eseguire nella struttura della directory durante il processo di ripristino.
  - Crea directory principale - Se l'immagine di backup acquisita contiene una struttura di directory principale, CA ARCserve D2D ricreerà la stessa struttura di directory nel percorso di destinazione di ripristino.

    Se l'opzione Crea directory principale non è selezionata, il file o la cartella da ripristinare verranno ripristinati direttamente nella cartella di destinazione.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt e C:\Folder1\SubFolder2\B.txt e durante il ripristino è stata specificata la destinazione D:\Restore.

    Se si sceglie di ripristinare i file A.txt e B.txt individualmente, la destinazione dei file ripristinati corrisponderà a D:\Restore\A.txt e "D:\Restore\B.txt. La directory principale al di sopra del livello di file specificato non verrà ricreata.

    Se si sceglie di eseguire il ripristino a partire dal livello SubFolder2, la destinazione dei file ripristinati corrisponderà a D:\Restore\SubFolder2\A.txt e D:\Restore\SubFolder2\B.txt. La directory principale al di sopra del livello di cartella specificato non verrà ricreata.

    Se l'opzione Crea directory principale è selezionata, verrà ricreato l'intero percorso della directory principale per i file o le cartelle (compreso il nome del volume) nella cartella di destinazione. Se i file o le cartelle da ripristinare appartengono allo stesso nome del volume, il percorso della directory principale di destinazione non includerà tale nome del volume. Tuttavia, se i file o le cartelle da ripristinare appartengono a diversi nomi di volume, il percorso della directory principale di destinazione includerà il nome del volume.

    Esempio:

    Se durante il backup vengono acquisiti i file C:\Folder1\SubFolder2\A.txt, C:\Folder1\SubFolder2\B.txt, e E:\Folder3\SubFolder4\C.txt e durante il ripristino è stata specificata la destinazione di ripristino D:\Restore.

    Se si desidera ripristinare soltanto il file A.txt, la destinazione del file ripristinato corrisponderà a D:\Restore\ Folder1\SubFolder2\A.txt (verrà ricreata l'intera directory principale, eccetto il nome del volume).

    Se si esegue il ripristino di entrambi i file A.txt e B.txt, la destinazione dei file ripristinati corrisponderà a D:\Restore\C\Folder1\SubFolder2\A.txt e D:\Restore\E\Folder3\SubFolder4\C.txt (verrà ricreata l'intera directory principale, compreso il nome del volume).

- **Password di Crittografia** - Se i dati del punto di ripristino selezionato sono crittografati, potrebbe essere necessario specificare la password di crittografia.

  Se il ripristino viene eseguito sullo stesso computer su cui è stato eseguito il backup crittografato, la password non verrà richiesta. La password verrà richiesta se viene eseguito il ripristino su un computer diverso.

  Nota: le icone riportate di seguito indicano se il punto di ripristino contiene informazioni crittografate e se è richiesta l'immissione di una password per il ripristino.

  Punto di ripristino non crittografato:

  Punto di ripristino crittografato:

Fare clic su Avanti.

Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.

8. Verificare che le informazioni della finestra di dialogo Riepilogo di Ripristino siano corrette.

   Nota: se si desidera modificare le opzioni di ripristino specificate, fare clic su Indietro per tornare alla finestra di dialogo corrispondente.

   Fare clic su Fine.

Le opzioni di ripristino verranno applicate e verrà eseguito il recupero dei dati.

Recupero dei server di origine mediante ripristini bare metal

Dopo aver risolto i problemi o eseguito la manutenzione dei server di origine, Virtual Standby consente di eseguire il recupero dei server di origine all'ultimo stato corretto e di includere le modifiche incrementali verificatesi durante l'attivazione della snapshot del punto di ripristino.

Tale processo di recupero viene denominato recupero V2P (dal formato virtuale al formato fisico).

Il processo di recupero V2P sfrutta il ripristino bare metal di CA ARCserve D2D (BMR) per ripristinare i dati da computer virtuali a computer fisici. Il ripristino bare metal consiste nel ripristino di interi sistemi, inclusa la reinstallazione del sistema operativo e delle applicazioni software, quindi dei dati e delle impostazioni.

Per l'esecuzione di un ripristino BMR è necessario disporre

- Almeno un backup completo.
- Almeno 1 GB di RAM installato sul computer virtuale e il server di origine di cui si sta eseguendo il recupero.
- Se si desidera eseguire il recupero di computer virtuali VMware su computer virtuali VMware configurati come server fisici, verificare che gli strumenti VMware siano installati sul computer virtuale di destinazione.

Il ripristino dei dischi dinamici viene eseguito solo a livello del disco. Se il backup dei dati avviene su un volume locale che risiede su un disco dinamico, tale disco non potrà essere ripristinato durante il ripristino bare metal. In tal caso, per eseguire il ripristino durante il ripristino bare metal è necessario eseguire una delle attività seguenti e quindi eseguire il ripristino bare meta dal punto di ripristino copiato:

- Eseguire il backup su un volume di un'altra unità.
- Eseguire il backup su una condivisione remota.
- Copiare un punto di ripristino su una destinazione diversa.

Nota: se si esegue il ripristino bare metal su un disco dinamico, si consiglia di non eseguire operazioni di disco prima della procedura BMR (quali pulizia, eliminazione del volume, ecc.); in caso contrario la presenza del disco potrebbe non essere rilevata.

Il processo di ripristino bare metal non cambia, indipendentemente dal metodo utilizzato per la creazione dell'immagine del kit di avvio.

Per ulteriori informazioni sulla procedura di creazione di un'immagine ISO o di una chiave USB di ripristino bare metal, consultare la sezione Modalità di creazione di un kit di avvio nella Guida per l'utente di CA ARCserve D2D.

L'applicazione consente di ripristinare i dati utilizzando i metodi descritti nella tabella seguente:

Metodo di ripristino	**Ulteriori informazioni**
Recupero dei server di origine dai dati convertiti in computer virtuali Virtual Standby basati su Hyper-V.	Recupero dei server di origine utilizzando i dati tratti da computer virtuali Virtual Standby basati su Hyper-V (a pagina 150).
Recupero dei server di origine dai dati convertiti in computer virtuali Virtual Standby basati su VMware.	Recupero dei server di origine utilizzando i dati tratti da computer virtuali Virtual Standby basati su VMware (a pagina 156).

Gestione del menu delle operazioni di ripristino bare metal

Il menu Operazioni di ripristino bare metal comprende i seguenti tre tipi di operazioni:

- Operazioni specifiche del disco
- Operazioni specifiche di volume/partizione
- Operazioni specifiche di ripristino bare metal

Operazioni specifiche del disco:

Per eseguire operazioni di specifico del disco, selezionare l'intestazione del disco e fare clic su Operazioni.

Pulitura disco

Questa operazione viene utilizzata per la pulitura di tutte le partizioni di un disco:

- Si tratta di un metodo alternativo per l'eliminazione di tutti i volumi di un disco. L'operazione di pulitura disco consente di non eliminare ogni volume singolarmente.
- Viene utilizzata per l'eliminazione di partizioni non-Windows. A causa di una limitazione di VDS, non è possibile eliminare la partizione non-Windows dall'interfaccia utente. Sarà tuttavia possibile utilizzare l'operazione per eseguire la pulitura completa.

Nota: durante il ripristino bare metal, se il disco di destinazione dispone di partizioni non-Windows o di partizioni OEM, non sarà possibile selezionare la partizione ed eliminarla dall'interfaccia utente di ripristino bare metal. Solitamente, questo problema si verifica se è stato installato Linux/Unix sul disco di destinazione. Per risolvere il problema, eseguire una delle seguenti attività:

- Selezionare l'intestazione del disco nell'interfaccia utente di ripristino bare metal, quindi utilizzare l'operazione Pulitura disco per eliminare tutte le partizioni presenti sul disco.
- Aprire un prompt dei comandi e digitare Diskpart per aprire la console del comando Diskpart. Digitare quindi "select disk x" (x corrisponderà al numero di disco) e "clean" per eliminare tutte le partizioni sul disco.

Converti in MBR

Questa operazione consente di convertire un disco in MBR (Master Boot Record, Record di avvio principale). L'operazione è disponibile solamente quando il disco selezionato è un disco GPT (tabella di partizione GUID) e non sono presenti volumi sul disco.

Converti in GPT

Questa operazione viene utilizzata per convertire un disco in GPT. L'operazione è disponibile solamente quando il disco selezionato è un disco MBR e non sono presenti volumi sul disco.

Converti in disco di base

Questa operazione viene utilizzata per convertire un disco in un disco di base. L'operazione è disponibile solamente quando il disco selezionato è un disco dinamico e non sono presenti volumi sul disco.

Converti in disco dinamico

Questa operazione viene utilizzata per convertire un disco in un disco dinamico. L'operazione è disponibile soltanto quando il disco selezionato è un disco di base.

Disco in linea

Questa operazione viene utilizzata per rendere un disco in linea. L'operazione è disponibile soltanto quando il disco selezionato è in stato Non in linea.

Proprietà disco

Questa operazione viene utilizzata per visualizzare proprietà del disco dettagliate. L'operazione è sempre disponibile. Quando viene selezionata, verrà visualizzata la finestra di dialogo Proprietà disco.

Operazioni specifiche di volume/partizione:

Per eseguire operazioni di volume/partizione, selezionare l'area di testo del disco, quindi fare clic su Operazioni. Questo menu consente di creare nuove partizioni corrispondenti alle partizioni di disco del volume di origine.

Crea partizione primaria

Questa operazione consente di creare una partizione su un disco di base. È disponibile solamente quando l'area selezionata è uno spazio su disco non allocato.

Crea partizione logica

Questa operazione consente di creare una partizione logica su un disco MBR di base. È disponibile solamente quando l'area selezionata è una partizione estesa.

Crea partizione estesa

Questa operazione viene utilizzata per creare una partizione estesa su un disco MBR di base. È disponibile solamente quando il disco è un disco MBR e l'area selezionata è uno spazio su disco non allocato.

Crea partizione di sistema riservato

Questa operazione consente di creare la partizione di sistema riservato su un sistema firmware BIOS e genera una relazione di mapping con la partizione di sistema EFI di origine. L'operazione è disponibile soltanto quando viene eseguito il ripristino di un sistema UEFI in un sistema BIOS.

Nota: se precedentemente è stata eseguita una conversione da UEFI a un sistema compatibile con BIOS, utilizzare l'opzione Crea partizione di sistema riservato per il ridimensionamento del disco di destinazione.

Crea partizione del sistema EFI

Questa operazione viene utilizzata per creare la partizione di sistema EFI su un disco GPT di base. È disponibile solamente quando il firmware del computer di destinazione è UEFI e il disco selezionato è un disco GPT di base.

Nota: se precedentemente è stata eseguita la conversione da BIOS a un sistema compatibile con UEFI, utilizzare l'opzione Crea partizione del sistema EFI per il ridimensionamento del disco di destinazione.

Nota: i sistemi che supportano UEFI richiedono che la partizione di avvio sia anche presente su un disco GPT (Tabella di partizione GUID). Se si utilizza un disco MBR (record di avvio principale), è necessario eseguire la conversione del disco in un disco GPT, quindi utilizzare l'operazione Crea partizione del sistema EFI per il ridimensionamento del disco.

Ridimensiona volume

Questa operazione consente di ridimensionare un volume. Si tratta di un metodo alternativo di Windows Estendi volume/Riduci volume. È disponibile solamente quando l'area selezionata è una partizione di disco valida.

Elimina volume

Questa operazione consente di eliminare un volume. È disponibile solamente quando l'area selezionata è un volume valido.

Elimina partizione estesa

Questa operazione viene utilizzata per eliminare la partizione estesa. È disponibile solamente quando l'area selezionata è una partizione estesa.

Proprietà volume

Questa operazione viene utilizzata per visualizzare le proprietà del volume dettagliate. Quando viene selezionata questa operazione, viene visualizzata la finestra di dialogo Proprietà volume.

Operazioni specifiche di ripristino bare metal:

Queste operazioni sono specifiche del ripristino bare metal. Per eseguire operazioni di ripristino bare metal, selezionare l'intestazione del disco o l'area di testo del disco, quindi fare clic su Operazioni.

Esegui mapping del disco da

Questa operazione viene utilizzata per stabilire una relazione di mapping tra i dischi dinamici di origine e di destinazione. L'opzione è disponibile soltanto quando il disco selezionato è un disco dinamico.

Nota: quando viene eseguito il mapping su un altro disco, la capacità di ciascun volume di destinazione mappato deve essere uguale o superiore alla capacità del volume di origine corrispondente.

Esegui mapping del volume da

Questa operazione viene utilizzata per stabilire una relazione di mapping tra i volumi di base di origine e di destinazione. L'opzione è disponibile soltanto quando il volume selezionato è un volume di base.

Nota: quando viene eseguito il mapping su un altro disco, la capacità di ciascun volume di destinazione mappato deve essere uguale o superiore alla capacità del volume di origine corrispondente.

Conferma

Questa operazione è sempre disponibile. Tutte le operazioni vengono memorizzate nella cache e non modificano i dischi di destinazione fino alla selezione dell'operazione Conferma.

Reimposta

Questa operazione è sempre disponibile. L'operazione Reimposta viene utilizzata per abbandonare le operazioni e ripristinare il layout del disco sullo stato predefinito. L'operazione esegue la pulitura di tutte le operazioni memorizzate nella cache. Per reimpostazione si intende ricaricare le informazioni di layout del disco di origine e di destinazione dal file di configurazione e dal sistema operativo corrente, annullando le modifiche apportate dall'utente alle informazioni di layout del disco.

Recupero dei server di origine utilizzando i dati tratti da computer virtuali Virtual Standby basati su Hyper-V

L'applicazione consente di recuperare i server di origine utilizzando i dati di CA ARCserve D2D convertiti nei computer virtuali Virtual Standby basati su Hyper-V.

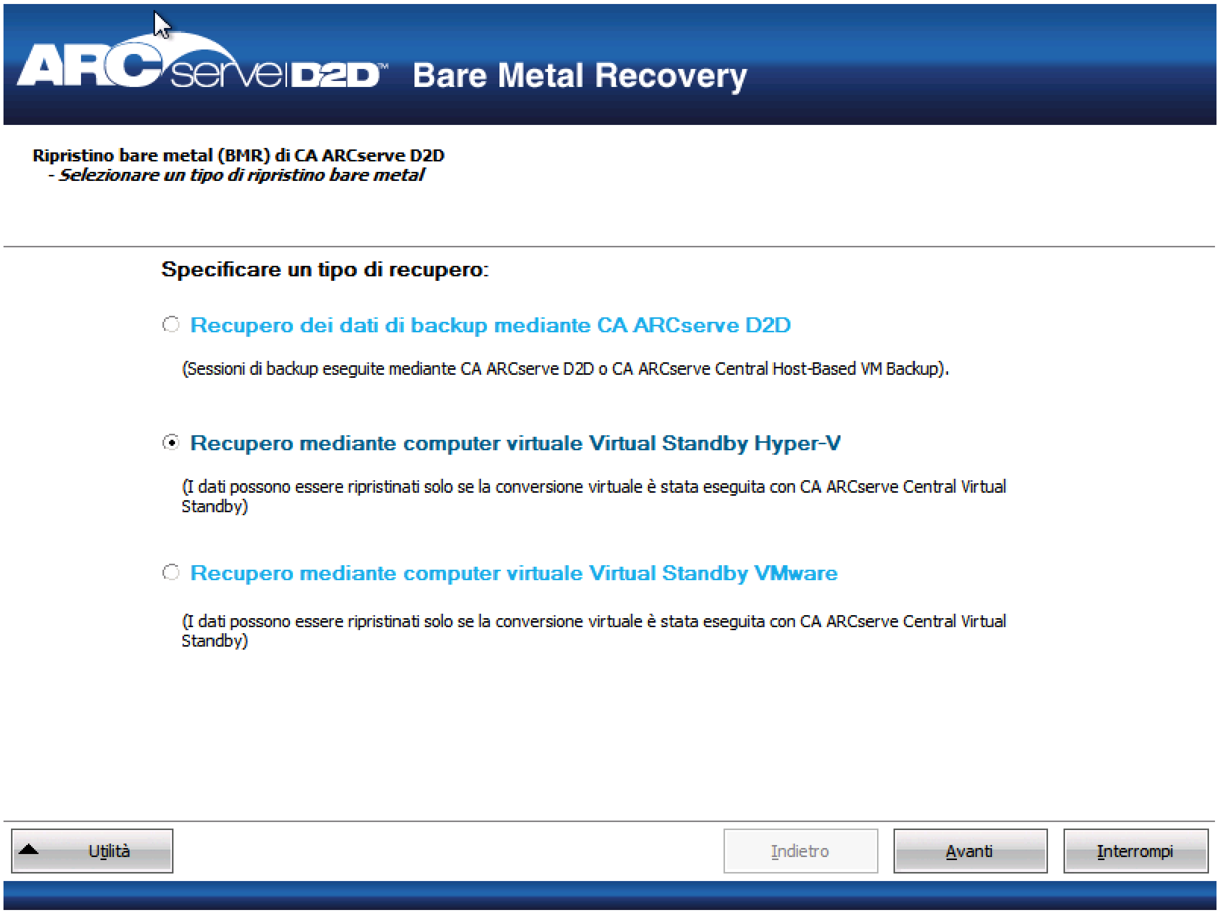
Nota: l'applicazione utilizza il processo di ripristino bare metal per recuperare i server di origine da computer virtuali Hyper-V. Per ulteriori informazioni, consultare la sezione Recupero dei server di origine mediante ripristini bare metal (a pagina 144).

CA ARCserve D2D consente di eseguire il ripristino bare metal dei computer V2P (dal formato virtuale al formato fisico). Questa funzionalità consente di eseguire il recupero V2P a partire dallo stato più recente di un computer virtuale di standby e ridurre, in tal modo, le perdite sul computer di produzione.

Dopo aver selezionato l'opzione Recupero mediante computer virtuale in standby Hyper-V, eseguire i seguenti passaggi prima di continuare la procedura di ripristino bare metal e completare il processo.

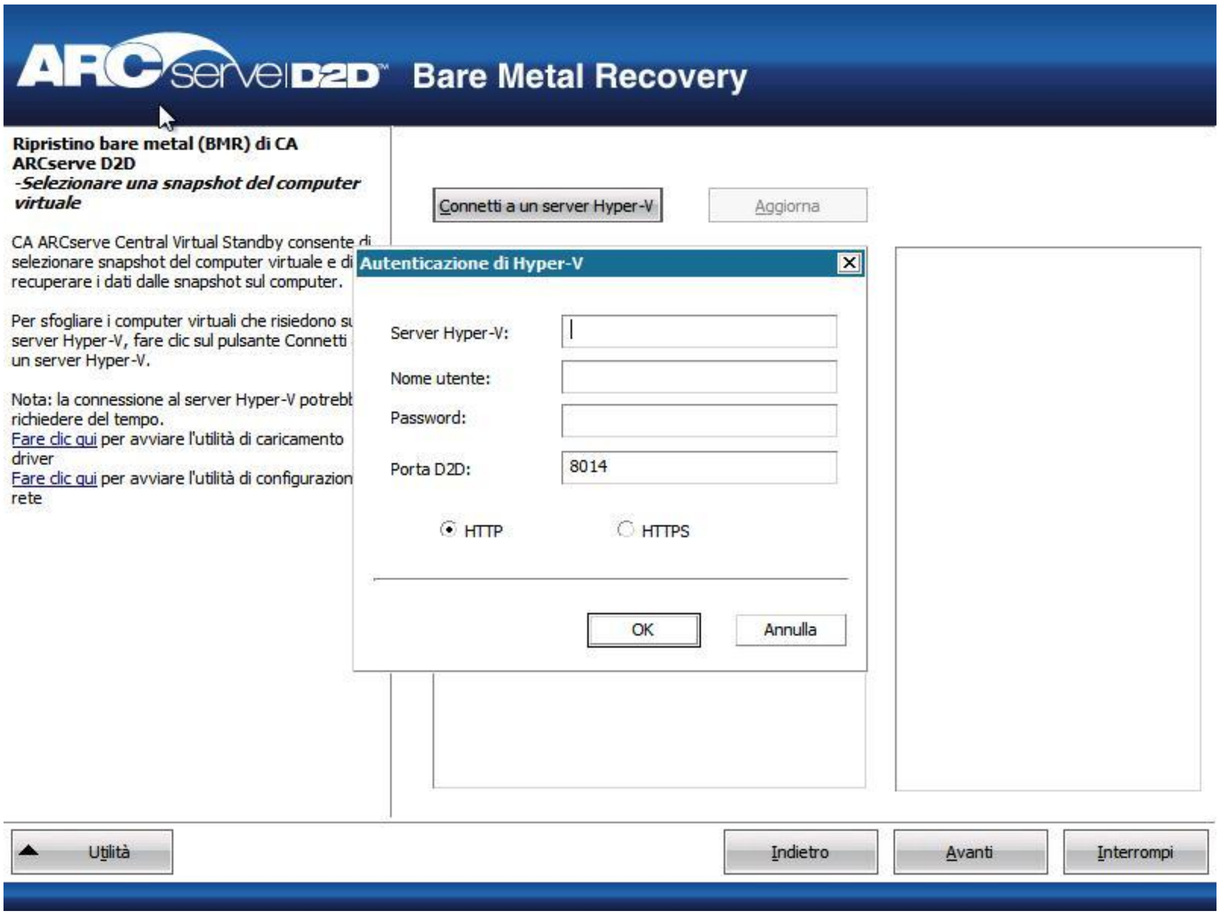
Procedere come descritto di seguito:

1. Dalla schermata della selezione guidata del tipo di ripristino bare metal (BMR), selezionare l'opzione Recupero mediante computer virtuale Virtual Standby Hyper-V.



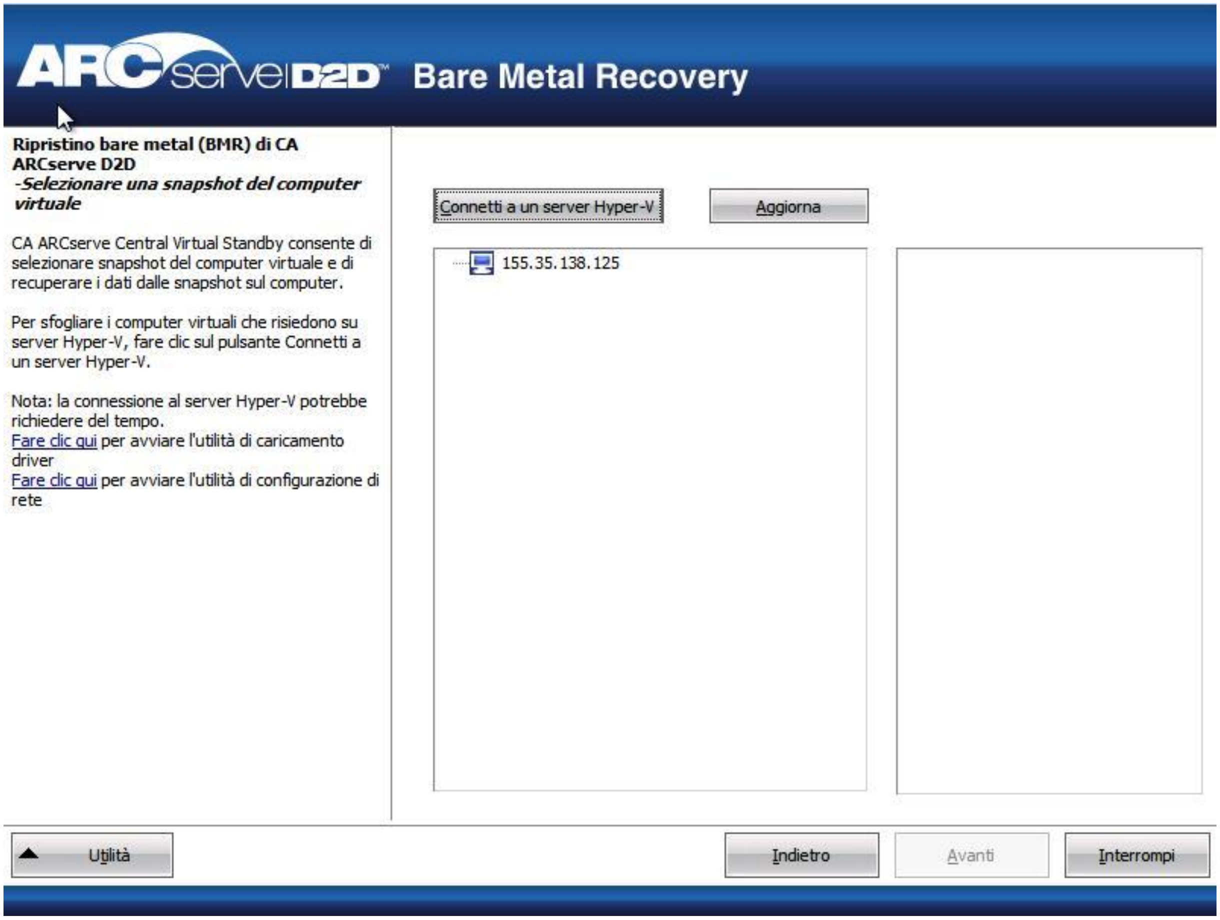
2. Fare clic su Avanti.

   Verrà visualizzata la schermata Selezionare una snapshot del computer virtuale con la finestra di dialogo Autenticazione di Hyper-V in cui vengono richiesti i dettagli relativi al server Hyper-v.



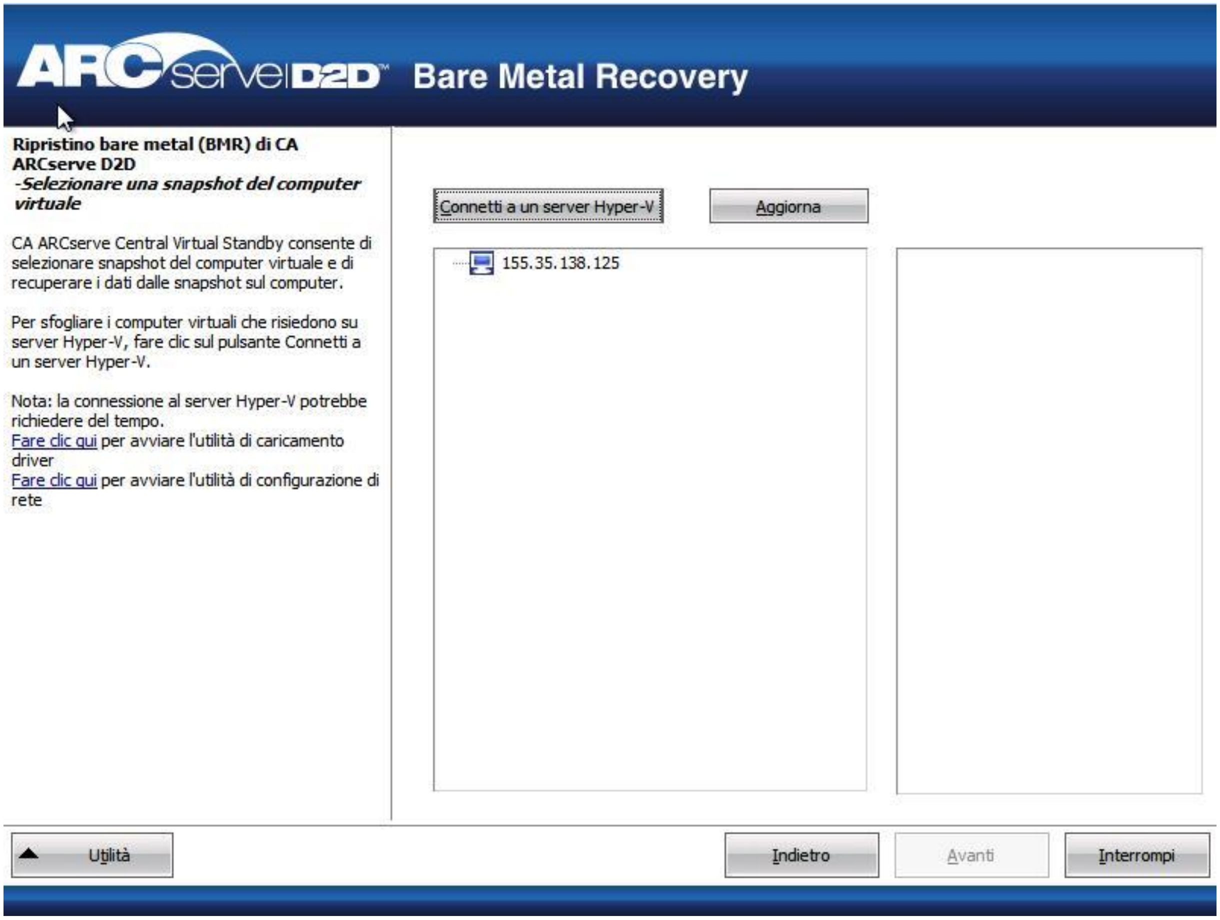
3. Immettere le informazioni di autenticazione e fare clic su OK.

   CA ARCserve D2D individua e visualizza il server Hyper-V con un elenco di tutti i computer virtuali che verranno convertiti sul server Hyper-V specificato mediante CA ARCserve Central Virtual Standby.



4. Selezionare il computer virtuale contenente le snapshot del punto di ripristino per l'immagine di backup.

   Verranno visualizzate le sessioni di backup (snapshot del punto di ripristino) del computer virtuale selezionato.



5. Selezionare la sessione di backup del computer virtuale (snapshot del punto di ripristino) che si desidera recuperare.

   Le informazioni relative alla snapshot del punto di ripristino selezionato (nome del computer virtuale, nome della sessione di backup, volumi di backup) verranno visualizzati nel riquadro di destra.

   Dopo aver selezionato uno dei punti di ripristino presenti nell'elenco, è possibile selezionare il punto di ripristino corrispondente allo Stato corrente o allo Stato più recente.

   - Se il computer virtuale utilizzato per il recupero viene acceso, verrà visualizzato lo stato corrente del punto di ripristino.
   - Se il computer virtuale utilizzato per il recupero viene spento, verrà visualizzato lo stato più recente del punto di ripristino.

     Se si seleziona Stato più recente per il punto di ripristino, verrà visualizzato un messaggio di errore per informare l'utente che il punto di ripristino utilizzato per il recupero corrisponde allo stato più recente (e non allo stato corrente). Inoltre, viene richiesto all'utente di avviare il computer virtuale per continuare il processo di recupero.

6. Verificare che il punto di ripristino selezionato sia corretto, quindi selezionare Avanti.

   Verrà visualizzata la scherma della procedura guidata di ripristino bare metal e le opzioni della modalità di recupero.

   Consultare la sezione Ripristino bare metal per completare i passaggi restanti della presente procedura e continuare dal passaggio di selezione della modalità di recupero.



Recupero dei server di origine utilizzando i dati tratti da computer virtuali Virtual Standby basati su VMware

L'applicazione consente di recuperare i server di origine utilizzando i dati di CA ARCserve D2D convertiti nei computer virtuali Virtual Standby basati su VMware.

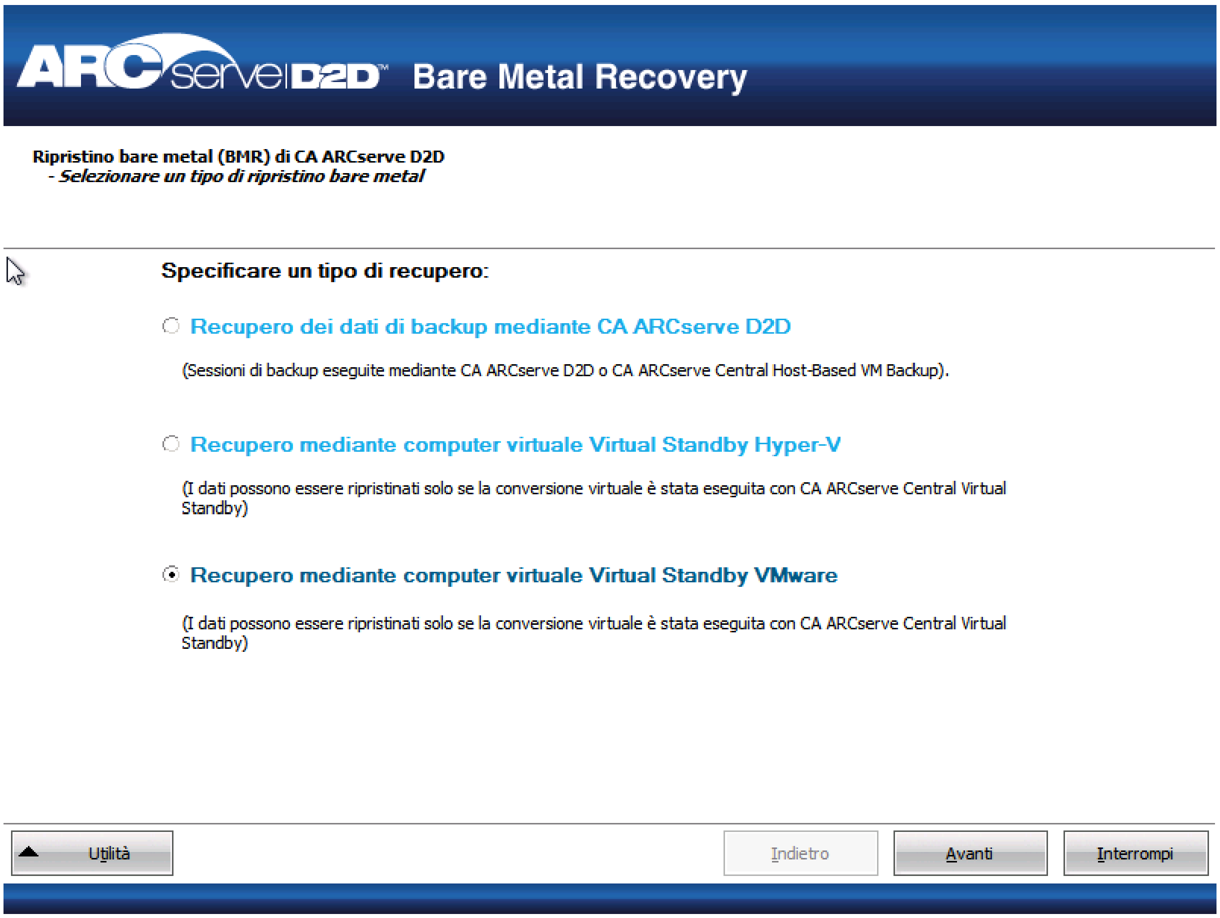
Nota: l'applicazione utilizza il processo di ripristino bare metal per recuperare i server di origine da computer virtuali VMware. Per ulteriori informazioni, consultare la sezione Recupero dei server di origine mediante ripristini bare metal (a pagina 144).

CA ARCserve D2D consente di eseguire il ripristino bare metal dei computer V2P (dal formato virtuale al formato fisico). Questa funzionalità consente di eseguire il recupero V2P a partire dallo stato più recente di un computer virtuale di standby e ridurre, in tal modo, le perdite sul computer di produzione.

Dopo aver selezionato l'opzione Recupero mediante computer virtuale in standby VMware, eseguire i seguenti passaggi prima di continuare la procedura di ripristino bare metal e completare il processo.

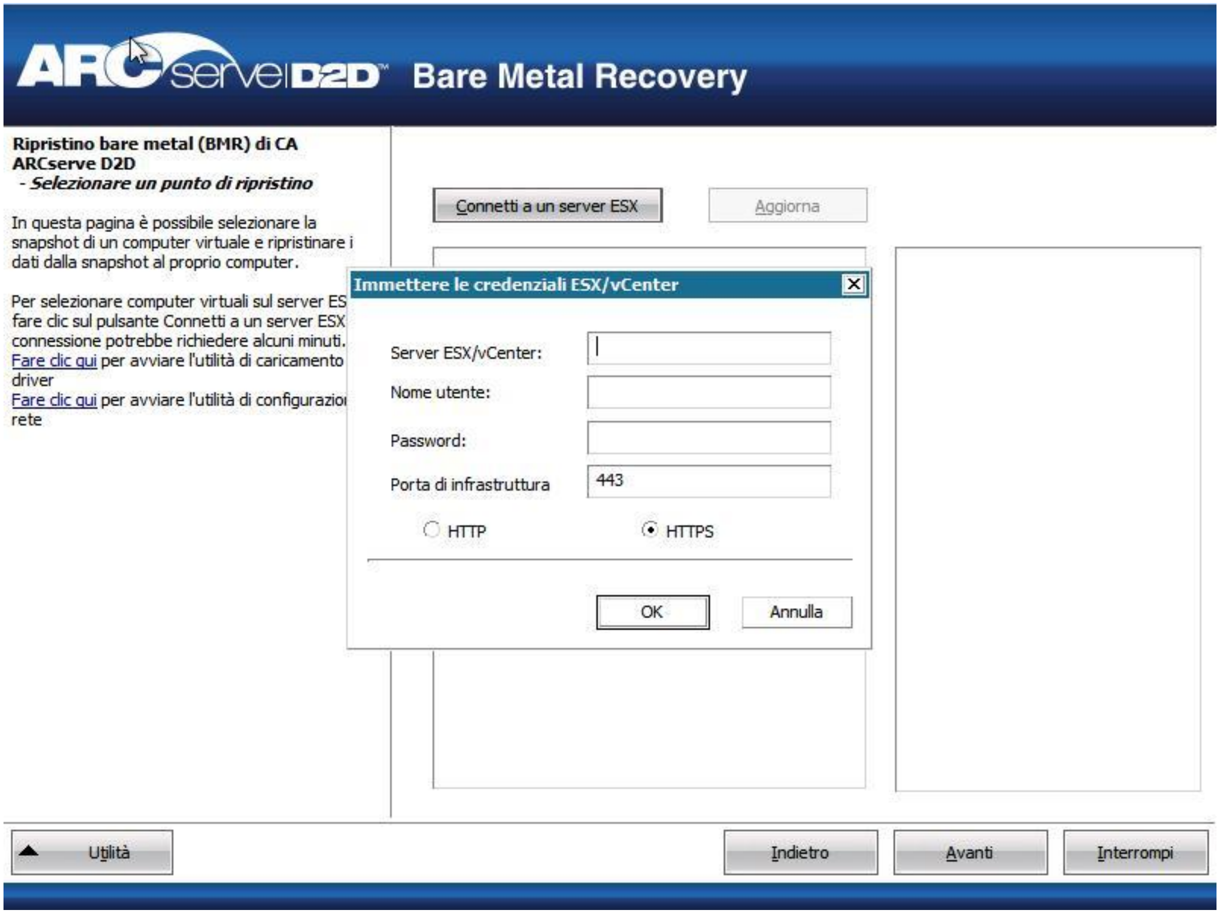
Procedere come descritto di seguito:

1. Dalla schermata della selezione guidata del tipo di ripristino bare metal (BMR), selezionare l'opzione Recupero mediante computer in standby virtuale VMware.



2. Fare clic su Avanti.

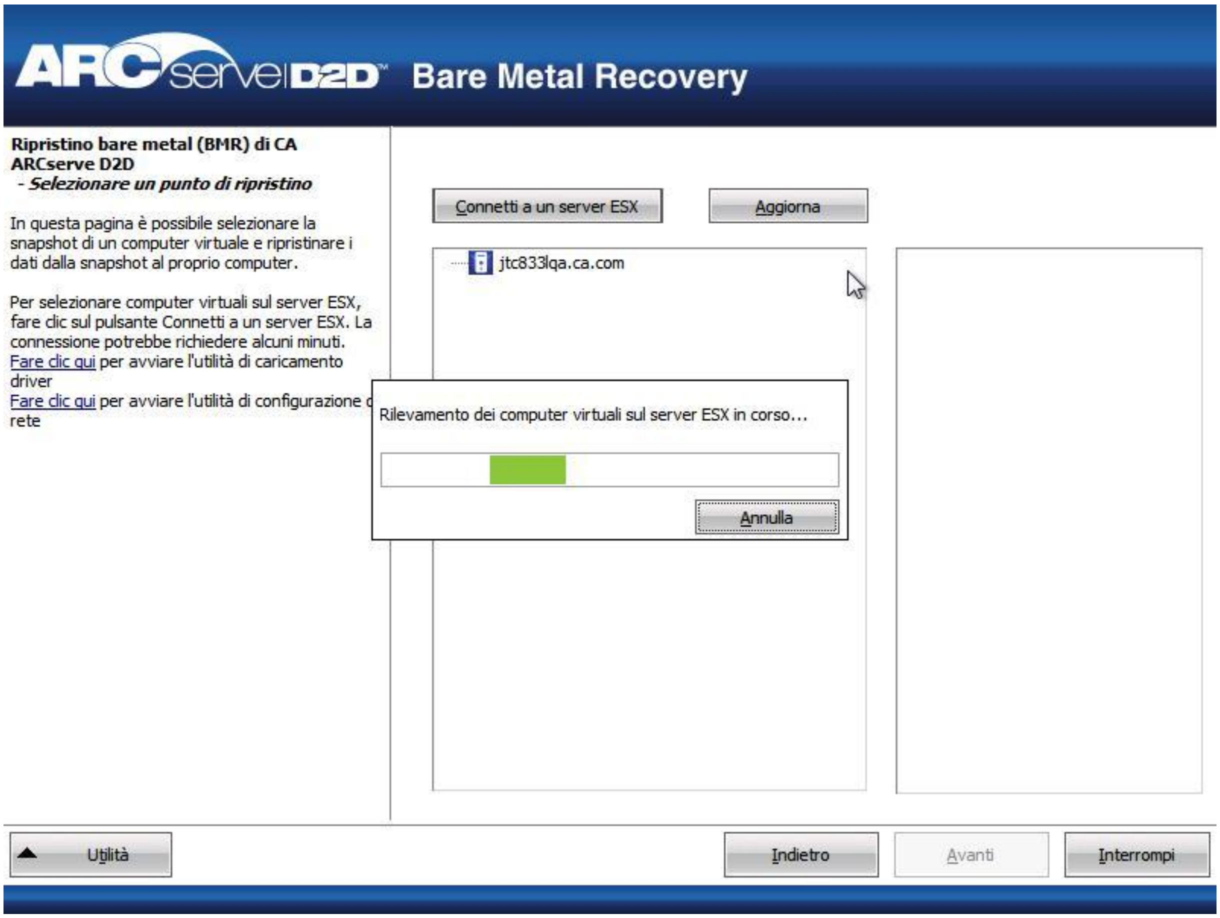
   Verrà visualizzata la schermata Selezionare un punto di ripristino con la finestra di dialogo delle credenziali di ESX/VC.



3. Immettere le informazioni per l'accesso e fare clic su OK.

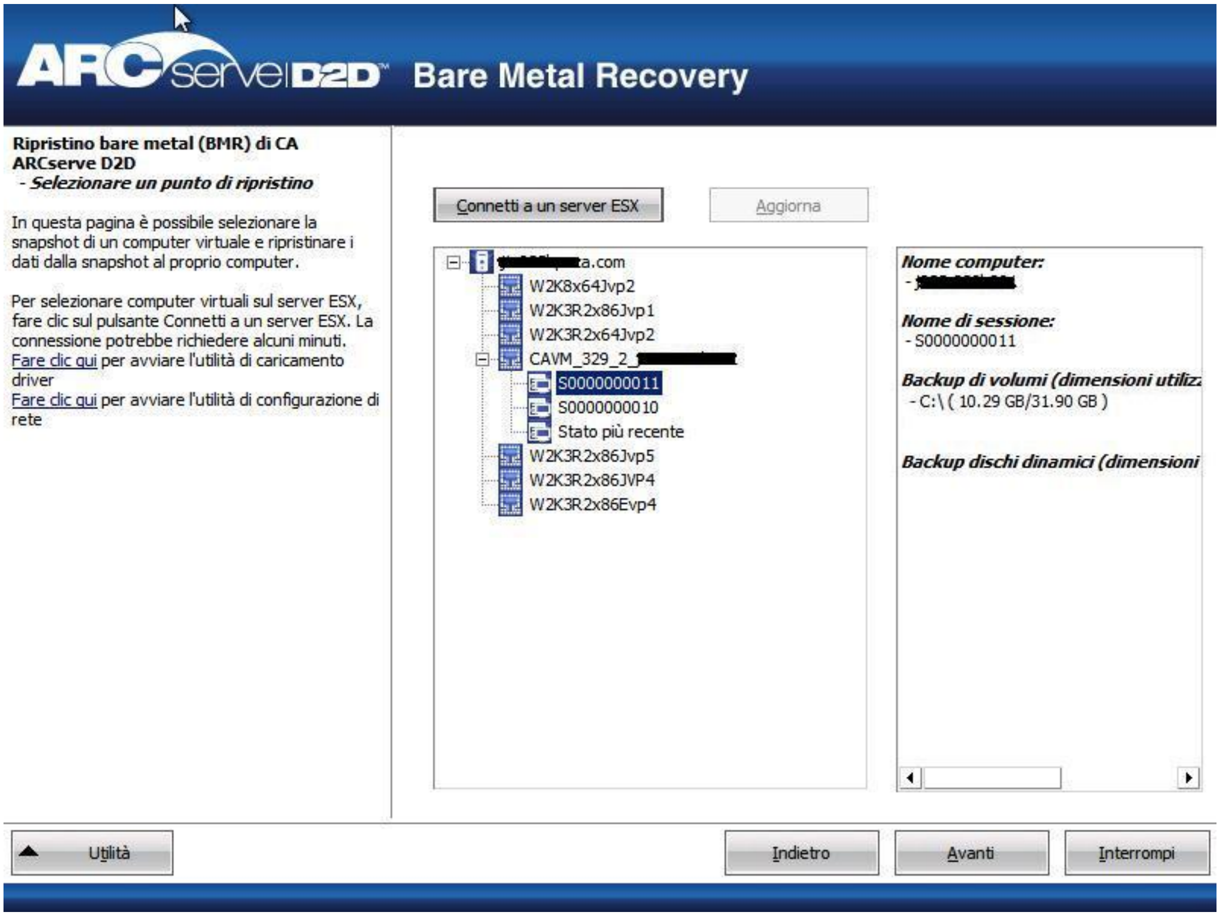
   Verrà visualizzata la schermata Selezionare un punto di ripristino.

   CA ARCserve D2D recupera tutte le snapshot del punto di ripristino per il server VMware selezionato e visualizza nel riquadro di sinistra, il server con un elenco di tutti i computer virtuali che risiedono sul server VMware selezionato.



4. Selezionare il computer virtuale contenente i punti di ripristino per l'immagine di backup.

   Verranno visualizzate le sessioni di backup (snapshot del punto di ripristino) del computer virtuale selezionato.



5. Selezionare la sessione di backup del computer virtuale (snapshot del punto di ripristino) che si desidera recuperare.

   Le informazioni relative alla snapshot del punto di ripristino selezionato (nome del computer virtuale, nome della sessione di backup, volumi di backup, dischi dinamici di backup) verranno visualizzate nel riquadro di destra.

   Dopo aver selezionato uno dei punti di ripristino presenti nell'elenco, è possibile selezionare il punto di ripristino corrispondente allo Stato corrente o allo Stato più recente.

   - Se il computer virtuale utilizzato per il recupero viene acceso, verrà visualizzato lo stato corrente del punto di ripristino.
   - Se il computer virtuale utilizzato per il recupero viene spento, verrà visualizzato lo stato più recente del punto di ripristino.

     Se si seleziona Stato più recente per il punto di ripristino, verrà visualizzato un messaggio di errore per informare l'utente che il punto di ripristino utilizzato per il recupero corrisponde allo stato più recente (e non allo stato corrente). Inoltre, viene richiesto all'utente di avviare il computer virtuale per continuare il processo di recupero.

6. Verificare che il punto di ripristino selezionato sia corretto, quindi selezionare Avanti.

   Viene visualizzata la scherma della procedura guidata di ripristino bare metal e le opzioni della modalità di recupero.

   Consultare la sezione Ripristino bare metal per completare i passaggi restanti della presente procedura e continuare dal passaggio di selezione della modalità di recupero.



Ripristino dei messaggi di posta elettronica di Microsoft Exchange

Virtual Standby consente di eseguire il ripristino di dati Microsoft Exchange dai punti di ripristino di CA ARCserve D2D. Dai punti di ripristino è possibile recuperare o ripristinare caselle di posta, cartelle della casella di posta e singoli messaggi di posta elettronica.

Nota: per eseguire ripristini granulari dei dati del server Exchange, l'account deve disporre dei requisiti di accesso necessari. Per ulteriori informazioni, consultare la *Guida per l'utente di CA ARCserve D2D*.

Per ripristinare messaggi di posta elettronica di Microsoft Exchange

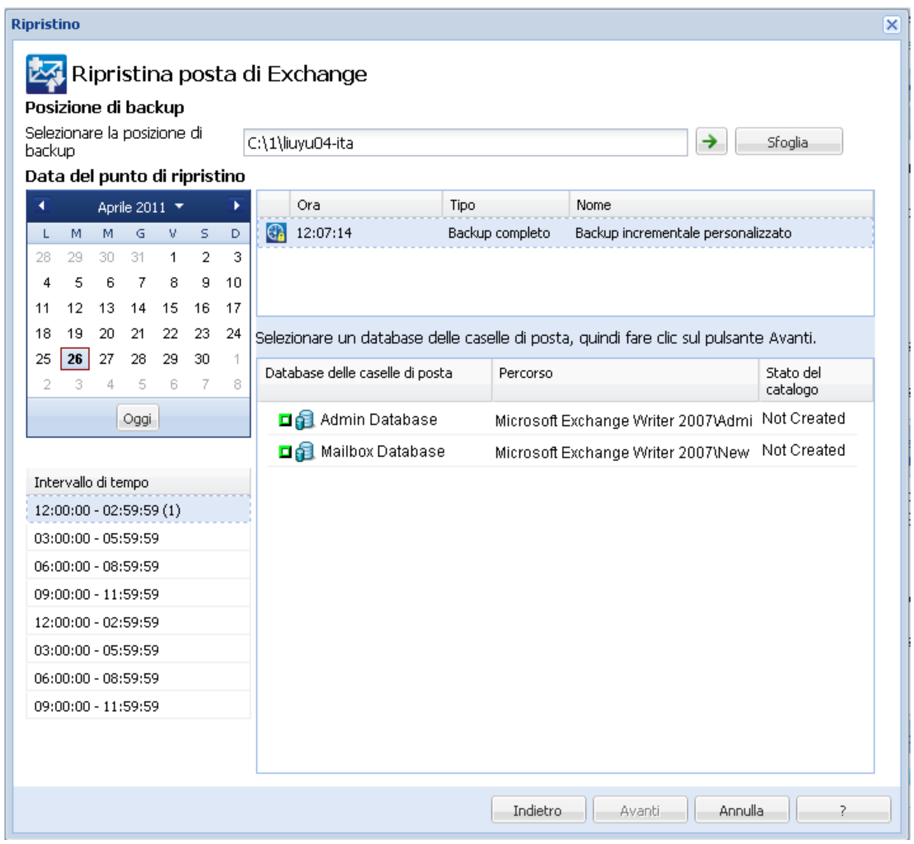
1. Accedere all'applicazione e fare clic su Nodo sulla barra di navigazione.

   Dalla schermata Nodo, espandere il gruppo contenente il nodo da ripristinare.

   Fare clic sulla casella di controllo accanto al nodo da ripristinare e selezionare Ripristina dalla barra degli strumenti.

2. Dalla finestra di dialogo Ripristino, fare clic su Ripristina posta di Exchange.

   Verrà visualizzata la finestra di dialogo Ripristina posta di Exchange.



3. Specificare la posizione di backup. È possibile specificare una posizione oppure individuare il percorso di archiviazione delle immagini di backup. Se necessario, immettere le credenziali Nome utente e Password per poter accedere al percorso. Fare clic sull'icona di convalida con la freccia verde per verificare che l'accesso alla posizione di origine sia stato eseguito correttamente.

   La visualizzazione calendario evidenzierà (in verde) tutte le date relative al periodo di tempo contenente i punti di ripristino per l'origine di backup selezionata.

4. Nel calendario, selezionare la data dell'immagine di backup da ripristinare.

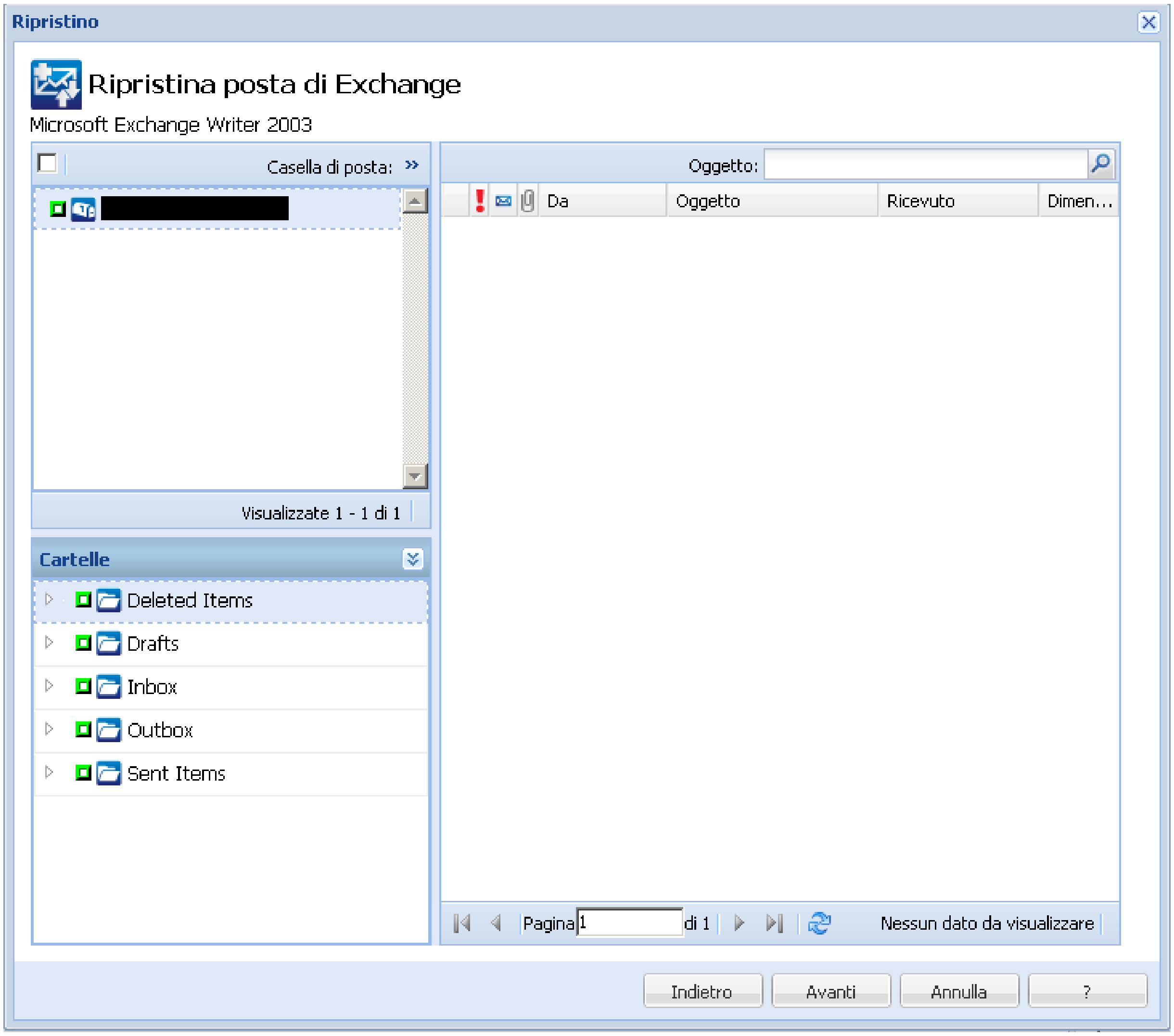
   Verranno visualizzati, quindi, i database delle caselle di posta Exchange associati alla data, unitamente all'ora di backup, al tipo di backup eseguito e al nome del backup.

5. Selezionare un database delle caselle di posta di Exchange da ripristinare, quindi fare clic su Avanti.

   Nota: se l'opzione di ripristino granulare di Exchange non è stata abilitata durante il backup, per cui non sono stati generati cataloghi, verrà visualizzato un messaggio di notifica in cui si richiederà di indicare se si desidera procedere alla generazione del catalogo di ripristino granulare di Exchange. Selezionando No, non sarà possibile sfogliare o selezionare un punto di ripristino granulare. Di conseguenza, sarà possibile eseguire esclusivamente un ripristino di database completo dalla finestra di dialogo Sfoglia punti di ripristino.

La finestra di dialogo Ripristina posta di Exchange viene aggiornata per visualizzare un elenco del contenuto della casella di posta elettronica per il database selezionato.

Nota: il ripristino granulare di Exchange supporta solo ripristini di posta elettronica. I ripristini di calendari, contatti, note e attività non sono supportati.



6. Selezionare il livello degli oggetti di Exchange da ripristinare (caselle di posta, cartelle o singoli messaggi).

   È possibile selezionare l'intero contenuto oppure parte del contenuto dell'oggetto di Exchange da ripristinare. È possibile selezionare più oggetti di Exchange da ripristinare.

   Nota: CA ARCserve D2D non supporta il ripristino granulare di oggetti di cartelle pubbliche di Exchange. Per eseguire il recupero dell'intero database di cartelle pubbliche, è necessario utilizzare il ripristino delle applicazioni, quindi estrarre l'oggetto Exchange specifico desiderato.

   Nota: quando si utilizza CA ARCserve D2D per il ripristino di singoli oggetti della casella di posta dal database delle caselle di posta di Exchange, il sistema operativo utilizzato per il ripristino deve coincidere con quello utilizzato per il backup (compreso lo stesso numero di versione di Windows, lo stesso livello di Service Pack, la versione corrispondente al pacchetto ridistribuibile Visual C++ richiesto per il supporto).

   Nota: durante l'esplorazione e il ripristino di messaggi di posta elettronica dall'interfaccia utente di CA ARCserve D2D, la proprietà del campo Da del messaggio potrebbe non essere visualizzata nell'interfaccia per le caselle di posta che non hanno mai effettuato la connessione a Exchange Server. Se ciò si verifica, i messaggi di posta elettronica verranno comunque ripristinati correttamente.

   a. È possibile selezionare un database delle caselle di posta.

      Selezionando un database delle caselle di posta, verranno ripristinate tutte le caselle di posta di quel database.

   b. L'utente potrà selezionare la casella di posta (o le caselle di posta) da ripristinare.

      Selezionando il livello casella di posta, verrà ripristinato tutto il contenuto (cartelle e messaggi di posta) della casella di posta selezionata.

   c. L'utente potrà selezionare una cartella da ripristinare all'interno di una determinata casella di posta.

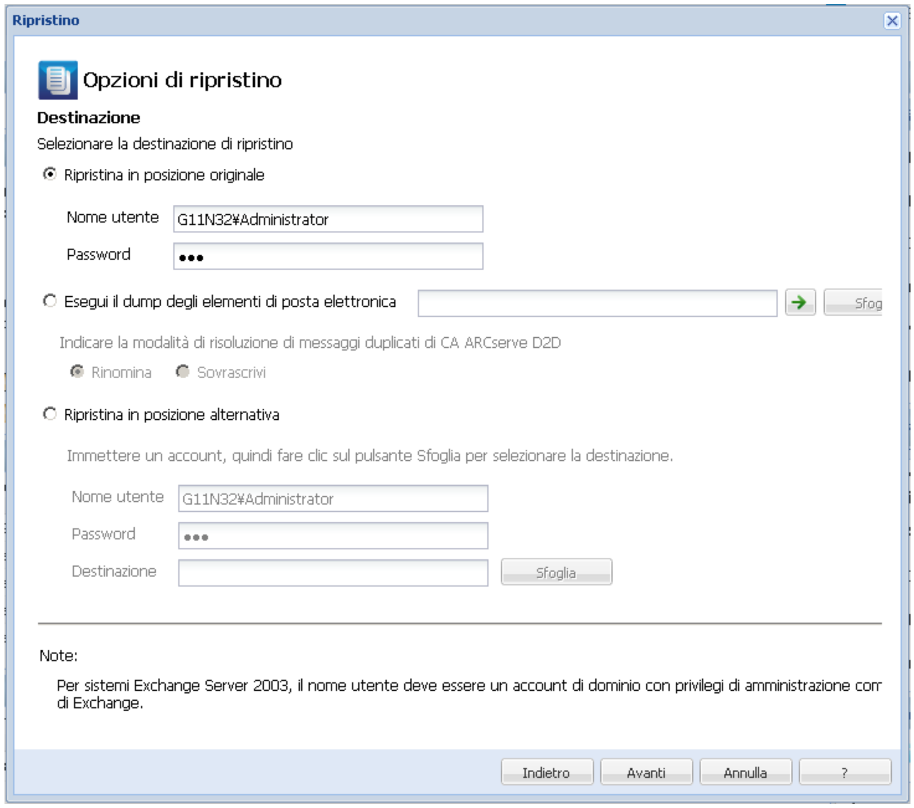
      Selezionando il livello cartella della casella di posta, verrà ripristinato tutto il contenuto di posta della cartella selezionata.

   d. L'utente potrà selezionare i singoli messaggi da ripristinare.

      Selezionando il livello messaggio singolo, verrà ripristinato solo l'oggetto di posta selezionato.

      Nota: solo su Exchange 2003, se i singoli messaggi da ripristinare sono stati inviati mediante un client di posta elettronica diverso da Outlook e il messaggio contiene un flag di stato, il messaggio verrà ripristinato, ma il flag non verrà incluso nel ripristino.

7. Dopo aver specificato gli oggetti di Exchange da ripristinare, fare clic su Avanti.



8. Selezionare la destinazione per il ripristino.

   Le opzioni disponibili consentono di eseguire il ripristino nella posizione originale del backup, oppure di eseguire il ripristino in una posizione diversa.

   Nota: per Exchange 2010, non è possibile procedere al ripristino in posizione originale degli elementi della casella di posta archiviati. Gli elementi della casella di posta archiviati possono essere ripristinati solo in posizione alternativa o su un disco locale. Inoltre, non è possibile ripristinare gli elementi standard della casella di posta in caselle di posta di archiviazione.

Ripristina in posizione originale

Consente di eseguire il ripristino dei messaggi di posta elettronica nella posizione originale di acquisizione dell'immagine di backup. I messaggi manterranno la stessa gerarchica e verranno ripristinati nella casella di posta e nella cartella originali.

- Se il computer corrente non è il server attivo di Exchange, CA ARCserve D2D rileverà la posizione del server attivo su cui eseguirà il ripristino dei messaggi di posta.
- Se la casella di posta è stata spostata su un altro server Exchange della stessa organizzazione, CA ARCserve D2D rileverà il nuovo server Exchange su cui risiede la casella di posta originale ed eseguirà il ripristino su tale server.
- Se il nome visualizzato per la casella di posta è stato modificato, qualsiasi tentativo di ripristino della casella di posta in posizione originale (da una precedente sessione di backup) non potrà essere completato, in quanto CA ARCserve D2D non sarà in grado di individuare il nome modificato. Per risolvere il problema, è possibile scegliere di ripristinare la casella di posta in posizione alternativa.

Nota: durante il ripristino di una casella di posta o di un messaggio di posta elettronica sulla posizione originale, verificare che la casella di posta di destinazione sia disponibile. In caso contrario, il ripristino avrà esito negativo. CA ARCserve D2D convalida la destinazione solo quando il processo di ripristino viene inoltrato.

Solo file di dettagli

Esegue il ripristino dei messaggi di posta elettronica su un disco. La posizione di disco può essere locale o corrispondere a un computer remoto. I messaggi ripristinati manterranno la stessa gerarchia della casella di posta di Exchange. Il nome del file viene utilizzato come oggetto del messaggio di posta elettronica.

Nota: se l'oggetto del messaggio di posta, il nome della cartella o il nome della casella di posta contengono i caratteri \/: *?, tali caratteri verranno sostituiti da un trattino (-) nel nome file. " < > |

Per questa opzione, sarà necessario specificare le azioni di CA ARCserve D2D in caso di conflitto. Exchange, consente di utilizzare lo stesso nome per più oggetti di messaggio contenuti nella stessa cartella. Tuttavia, i file system non possono contenere due file con lo stesso nome in una stessa cartella.

Esistono due opzioni per la risoluzione di questo conflitto:

- **Rinomina** - Se sul disco è presente un file con lo stesso nome dell'oggetto del messaggio di posta, CA ARCserve D2D aggiungerà un numero alla fine dell'oggetto del messaggio di posta.
- **Sovrascrivi** - Se sul disco è presente un file con lo stesso nome dell'oggetto del messaggio di posta, CA ARCserve D2D sovrascriverà il file.

Nota: quando si selezionano singoli oggetti di posta elettronica per l'esecuzione del ripristino su disco (dump), per impostazione predefinita il formato dell'oggetto di posta elettronica ripristinato corrisponderà a un file di messaggio Outlook (.msg) e non a un file Personal Storage Table (.pst).

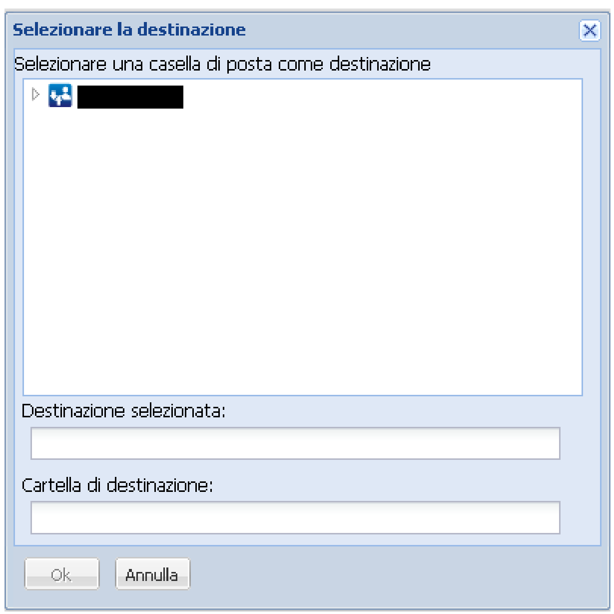
Ripristina in posizione alternativa:

Ripristina i messaggi in un percorso specificato o consente di individuare il percorso in cui ripristinare le immagini di backup. La destinazione deve essere una casella di posta facente parte della stessa organizzazione di Exchange. Sarà necessario specificare un nome per la nuova cartella. (Nei ripristini in posizione alternativa, la destinazione non può essere una cartella pubblica).

Nota: durante il ripristino di un messaggio di posta elettronica su una posizione alternativa, se la cartella di destinazione specificata è già esistente, il ripristino non verrà interrotto. Tuttavia, se la cartella specificata non esiste, CA ARCserve D2D creerà la cartella e procederà, quindi, con il ripristino.

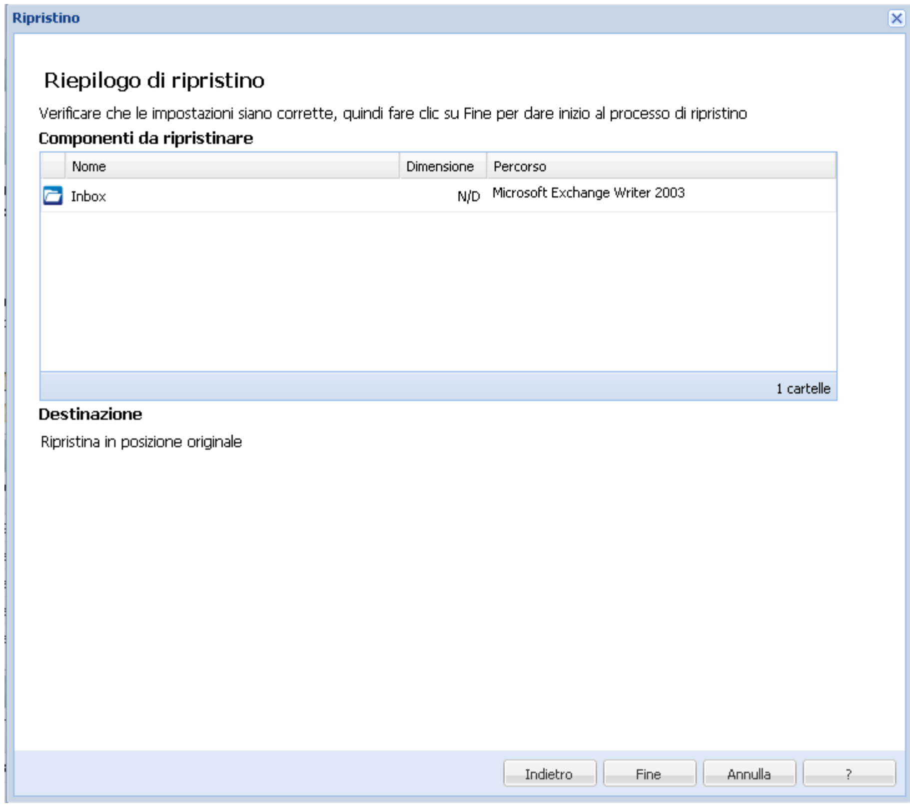
Dopo aver immesso il nome utente e la password, fare clic sul pulsante Sfoglia per visualizzare un elenco di tutti i server Exchange, dei gruppi di archiviazione, dei database di Exchange e delle caselle di posta presenti nell'organizzazione corrente.

Selezionare una casella di posta come destinazione.



9. Dopo aver selezionato le opzioni di ripristino, fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Riepilogo di ripristino.



10. Verificare che le opzioni di ripristino e le impostazioni siano corrette.

    - Se le informazioni di riepilogo non sono corrette, fare clic su Indietro e accedere alla finestra di dialogo corrispondente per modificare le impostazioni non corrette.
    - Se le informazioni di riepilogo sono corrette, fare clic su Fine per avviare il processo di ripristino.

    Nota: se il processo di generazione catalogo e di ripristino granulare di Exchange è in esecuzione, la sessione di backup sarà in stato montato. Non eseguire alcuna operazione (formattazione, modifica della lettera di unità, eliminazione della partizione, ecc.) sul volume montato.

Capitolo 8: Risoluzione dei problemi di CA ARCserve Central Virtual Standby

In questa sezione vengono fornite informazioni che consentono di identificare e risolvere i problemi che possono verificarsi durante l'utilizzo di CA ARCserve Central Virtual Standby.

Questa sezione contiene i seguenti argomenti:

Messaggi di errore di connessione al server specificato durante il tentativo di aggiunta dei nodi.

Valido per piattaforme Windows.

Sintomo:

Quando si tenta di aggiungere o di stabilire la connessione a nodi dalla schermata Nodo, viene visualizzato il seguente messaggio di errore.

```
Impossibile connettersi al server specificato.
```

Soluzione:

Se viene visualizzato il messaggio riportato sopra quando si tenta di aggiungere nodi dalla schermata Nodo, le seguenti azioni correttive possono contribuire alla risoluzione del problema:

- Verificare che il servizio Windows Server sia in esecuzione sul server CA ARCserve Central Virtual Standby e sul computer virtuale (nodo) di origine.
- Assicurarsi che sia applicata un'eccezione di Windows Firewall al servizio Condivisione file e stampanti di Windows sul server CA ARCserve Central Virtual Standby e sul computer virtuale (nodo) di origine.
- Assicurarsi che un'eccezione di Windows Firewall sia applicata al servizio Netlogon di Windows solo se il nodo non è membro di un dominio. Eseguire questa attività sul server CA ARCserve Central Virtual Standby sul computer virtuale (nodo) di origine.

- Verificare che il valore applicato al modello Condivisione e protezione per l'account locale sia Classico. Per applicare il valore Classico, procedere come segue:

  Nota: eseguire i seguenti passaggi sul server CA ARCserve Central Virtual Standby e sul computer virtuale (nodo) di origine.

  1. Accedere al server CA ARCserve Central Virtual Standby e aprire il Pannello di controllo.
  2. Dal Pannello di controllo selezionare Strumenti di amministrazione.
  3. Fare doppio clic su Criteri di protezione locali.

     Verrà visualizzata la finestra di dialogo Criteri di protezione locali.

  4. Dalla finestra Criteri di protezione locali, espandere Criteri locali e Opzioni di protezione.

     Verranno visualizzati i criteri di protezione.

  5. Fare clic con il pulsante destro del mouse su Accesso alla rete: modello di condivisione e protezione per gli account locali e scegliere Proprietà dal menu di scelta rapida.

     Verrà visualizzata la finestra delle proprietà Accesso alla rete: modello di condivisione e protezione per gli account locali.

  6. Fare clic su Impostazioni di protezione locali.

     Dall'elenco a discesa, selezionare Classico: gli utenti locali effettuano l'autenticazione di se stessi.

     Fare clic su OK.

- Verificare che il valore applicato ai criteri locali per il livello di autenticazione del manager della rete LAN sia impostato su invia LM & NTLMv2 – utilizza la protezione di sessione NTLMv2 se negoziata. Per applicare il valore, eseguire le seguenti operazioni:

  1. Accedere al server CA ARCserve Central Virtual Standby e aprire il prompt dei comandi.

     Eseguire il seguente comando

     `secpol.msc`

     Verrà visualizzata la finestra di dialogo Impostazioni protezione locale.

  2. Selezionare i criteri locali e fare clic sulle opzioni di protezione.

     Ricerca di protezione di rete: livello di autenticazione di manager rete LAN.

     Fare doppio clic sull'opzione.

     Verrà visualizzata la finestra di dialogo Proprietà.

3. Selezionare l'opzione seguente e fare clic su OK.

   `invia LM & NTLMv2 – utilizza la protezione di sessione NTLMv2 se negoziata.`

4. Dal prompt dei comandi, eseguire il comando riportato di seguito:

   `gpupdate`

Il valore viene applicato.

Pagine Web vuote o errori Javascript.

Valido sui sistemi operativi Windows Server 2008 e Windows Server 2003.

Sintomo:

Quando i siti Web di CA ARCserve Central Applications vengono aperti utilizzando Internet Explorer, vengono visualizzate pagine Web vuote oppure si verificano errori Javascript. Il problema si verifica quando si apre Internet Explorer sui sistemi operativi Windows Server 2008 e Windows Server 2003.

Questo problema si verifica nei seguenti casi:

- Quando si utilizza Internet Explorer 8 o Internet Explorer 9 per visualizzare l'applicazione e il browser non riconosce l'URL come sito attendibile.
- Quando si utilizza Internet Explorer 9 per visualizzare l'applicazione e il protocollo di comunicazione in uso è HTTPS.

Soluzione:

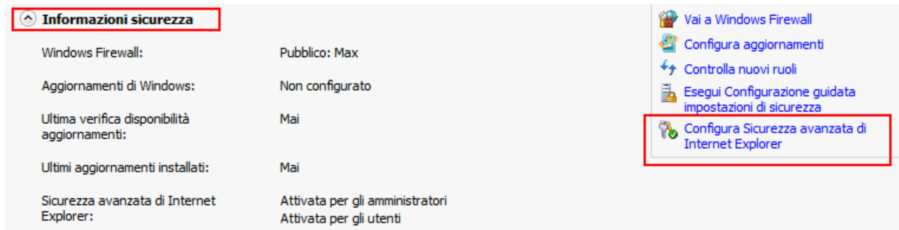
Per risolvere il problema, disattivare la protezione avanzata di Internet Explorer sui computer utilizzati per visualizzare l'applicazione.

Per disattivare la protezione avanzata di Internet Explorer su sistemi Windows Server 2008, procedere come segue:

1. Accedere al computer Windows Server 2008 utilizzato per visualizzare i rapporti utilizzando l'account di amministratore o un account che dispone di privilegi amministrativi.
2. Fare clic con il pulsante destro su Computer sul desktop e scegliere Gestisci per aprire la finestra di Server Manager.

3. Dalla finestra Server manager fare clic su Server Manager (nome server).

   Dalla sezione Riepilogo server, aprire Informazioni di protezione e fare clic su Configura Protezione avanzata di Internet Explorer, come illustrato a continuazione:

   Viene visualizzata la finestra di dialogo Protezione avanzata di Internet Explorer.

4. Nella finestra di dialogo Protezione avanzata di Internet Explorer, procedere come segue:

   - Disattiva il controllo Administrators--Click
   - Disattiva il controllo Users--Click

   Fare clic su OK.

La finestra di dialogo Protezione avanzata di Internet Explorer viene chiusa e la protezione di Internet Explorer viene disabilitata.

Per disattivare la protezione avanzata di Internet Explorer su sistemi Windows Server 2003, procedere come segue:

1. Accedere al computer Windows Server 2003 utilizzato per visualizzare i rapporti utilizzando l'account di amministratore o un account che dispone di privilegi amministrativi.
2. Aprire il Pannello di controllo di Windows, quindi aprire Installazione applicazioni.
3. Dalla finestra di dialogo Installazione applicazioni selezionare l'opzione Installazione componenti di Windows per avviare l'Aggiunta guidata componenti di Windows.

   Eliminare il segno di spunta accanto a Protezione avanzata di Internet Explorer.

   Fare clic su Avanti.

   Proseguire seguendo le istruzioni visualizzate per completare l'installazione, quindi fare clic su Fine.

La protezione avanzata di Internet Explorer è disabilitata.

Risoluzione dei problemi relativi al caricamento delle pagine

Valido per piattaforme Windows.

Sintomo:

La finestra del browser visualizza i messaggi di errore riportati di seguito quando viene eseguito l'accesso ai nodi CA ARCserve Central Applications e CA ARCserve D2D e ai server di monitoraggio.

Messaggio 1:

`Gli errori presenti nella pagina Web potrebbero impedirne il corretto funzionamento.`

Messaggio 2:

`!`

Soluzione:

Il caricamento delle pagine Web non viene eseguito correttamente per diverse ragioni. Nella tabella seguente sono descritte le cause più comuni e le corrispondenti misure correttive:

Motivo	Misura correttiva
Si sono verificati problemi relativi al codice sorgente HTML sottostante.	Aggiornare la pagina Web e riprovare.
La rete blocca l'esecuzione degli script attivi, i controlli ActiveX o i programmi Java.	Consentire al browser di utilizzare gli script attivi, i controlli ActiveX o i programmi Java.
L'applicazione antivirus è configurata per la scansione dei file temporanei Internet e dei programmi scaricati.	Applicare un filtro nell'applicazione antivirus in modo da consentire i file Internet associati alle pagine Web di CA ARCserve Central Applications.
Il motore di script installato nel computer è danneggiato o non è aggiornato.	Aggiornare il motore di script.
I driver della scheda video installati nel computer sono danneggiati o non sono aggiornati.	Aggiornare i driver della scheda video.
Il componente DirectX installato nel computer è danneggiato o non è aggiornato.	Aggiornare il componente DirectX.

Le pagine Web non vengono caricate correttamente quando si accede ai nodi CA ARCserve D2D e ai server di monitoraggio

Valido per piattaforme Windows.

Sintomo:

Le pagine Web non vengono caricate correttamente nel browser e/o vengono visualizzati messaggi di errore quando si accede ai nodi CA ARCserve D2D e ai server di monitoraggio dalla schermata Nodi.

Soluzione:

Questo comportamento interessa principalmente i browser Internet Explorer. È possibile che le pagine Web non vengano caricate correttamente quando l'esecuzione script, i controlli ActiveX o i programmi Java sono disabilitati nel computer o bloccati sulla rete.

Per risolvere il problema, aggiornare la finestra del browser. Se il problema persiste dopo l'aggiornamento della finestra del browser, procedere come segue:

1. Aprire Internet Explorer.

   Scegliere Opzioni Internet dal menu Strumenti.

   Verrà visualizzata la finestra di dialogo Opzioni Internet.

2. Fare clic sulla scheda Protezione.

   Vengono visualizzate le opzioni di sicurezza.

3. Fare clic sull'area Internet.

   Vengono visualizzate le opzioni relative all'area Internet.

4. Fare clic su Livello personalizzato.

   Viene visualizzata la finestra di dialogo Impostazioni di sicurezza - Area Internet.

5. Scorrere fino alla categoria Esecuzione script.

   individuare Esecuzione script attivo.

   Selezionare l'opzione Attiva o Chiedi conferma.

6. Fare clic su OK nella finestra di dialogo impostazioni di sicurezza - Area Internet.

   La finestra di dialogo Impostazioni di sicurezza - Area Internet viene chiusa.

7. Fare clic su OK nella finestra di dialogo Opzioni Internet.

   La finestra di dialogo Opzioni Internet viene chiusa e l'opzione di esecuzione script attivo viene applicata.

Nota: se il problema non viene risolto, contattare l'amministratore di sistema per verificare che altri programmi, ad esempio programmi antivirus o firewall, non blocchino l'esecuzione degli script attivi, i controlli ActiveX o i programmi Java.

Visualizzazione di caratteri corrotti nella finestra del browser durante l'accesso a CA ARCserve Central Applications

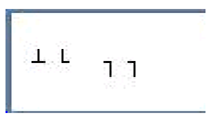
Valido per tutti i sistemi operativi Windows e per tutti i browser.

Sintomo:

Quando viene eseguito l'accesso a CA ARCserve Central Applications, vengono visualizzati caratteri corrotti nell'area di contenuto della finestra del browser.

Soluzione:

Questo problema si verifica nel caso in cui l'installazione di CA ARCserve Central Applications sia stata eseguita mediante comunicazione HTTPS e l'accesso a CA ARCserve Central Applications mediante comunicazione HTTP. Il componente dei servizi Web sottostanti di CA ARCserve Central Applications non supporta la funzionalità di conversione degli URL HTTP in HTTPS. Di conseguenza, i caratteri corrotti vengono visualizzati nella finestra del browser. Ad esempio:



Per correggere il problema, accedere a CA ARCserve Central Applications utilizzando il protocollo HTTPS per l'installazione o la configurazione delle applicazioni di comunicazione che utilizzano tale protocollo.

Errore del servizio Web di CA ARCserve D2D su nodi CA ARCserve D2D

Valido per piattaforme Windows.

Sintomo:

Il servizio Web in esecuzione sui nodi CA ARCserve D2D viene avviato e successivamente produce un errore oppure non viene avviato.

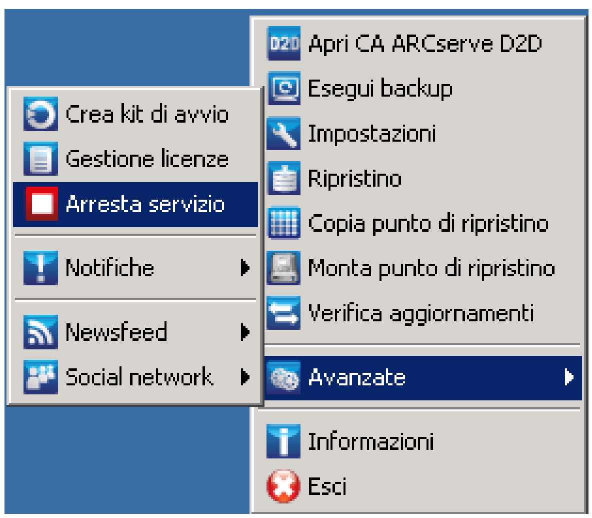
Soluzione:

Il problema si verifica quando la porta utilizzata dal servizio Web di CA ARCserve D2D coincide con quella utilizzata dal servizio Web VMware vCenter (Tomcat).

La porta utilizzata da CA ARCserve D2D potrebbe essere in conflitto con la porta predefinita utilizzata da Tomcat. In tal caso, se il server Tomcat viene avviato prima di CA ARCserve D2D potrebbero verificarsi errori. Per risolvere il problema, modificare la porta predefinita di Tomcat nel seguente modo:

1. Accedere a Computer di monitoraggio CA ARCserve D2D, fare clic sull'opzione Avanzate e selezionare Interrompi servizio.

   Il servizio Web di CA ARCserve D2D viene interrotto.

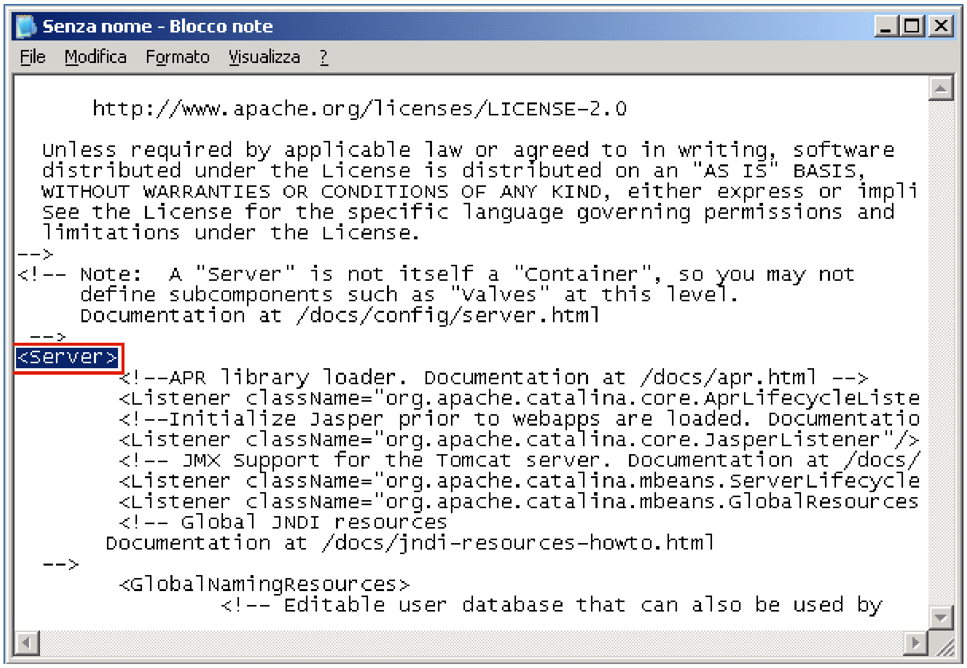
   

2. Aprire il file server.xml di Tomcat per modificare o configurare il comportamento di Tomcat.

   Il file server.xml di Tomcat è disponibile nel seguente percorso:

   `C:\Programmi\CA\ARCserve Central Applications\TOMCAT\conf`

3. Individuare il tag <Server> nel file server.xml.




```
     http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or impli
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- Note:  A "Server" is not itself a "Container", so you may not
     define subcomponents such as "Valves" at this level.
     Documentation at /docs/config/server.html
 -->
<Server>
        <!--APR library loader. Documentation at /docs/apr.html -->
        <Listener className="org.apache.catalina.core.AprLifecycleListe
        <!--Initialize Jasper prior to webapps are loaded. Documentatio
        <Listener className="org.apache.catalina.core.JasperListener"/>
        <!-- JMX Support for the Tomcat server. Documentation at /docs/
        <Listener className="org.apache.catalina.mbeans.ServerLifecycle
        <Listener className="org.apache.catalina.mbeans.GlobalResources
        <!-- Global JNDI resources
       Documentation at /docs/jndi-resources-howto.html
  -->
        <GlobalNamingResources>
                <!-- Editable user database that can also be used by
```

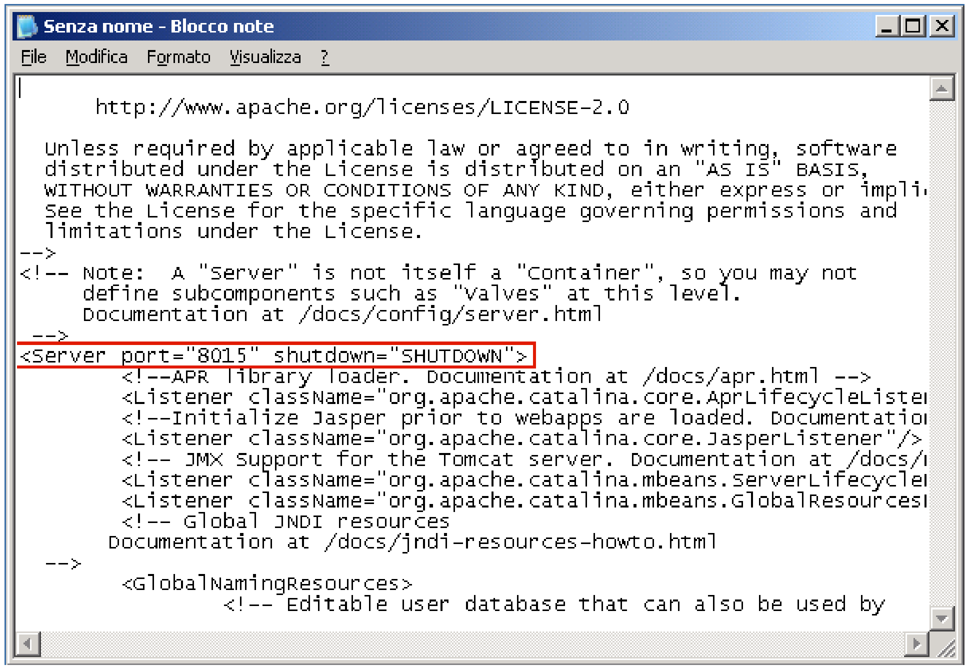
4. Modificare il tag <Server> nel seguente modo:

   Da:

   <Server>

   A:

   <Server port="8015" shutdown="SHUTDOWN">



5. Salvare e chiudere il file server.xml.

   Il comando di arresto del server Tomcat viene configurato per essere ricevuto dal server attraverso la porta specificata (8015).

6. Accedere a Computer di monitoraggio CA ARCserve D2D, fare clic sull'opzione Avanzate e selezionare Avvia servizio.

   Il servizio Web di CA ARCserve D2D viene avviato.

Lentezza di esecuzione del servizio Web di CA ARCserve D2D

Applicabile ai sistemi operativi Windows.

Sintomo 1:

L'esecuzione del servizio Web di CA ARCserve D2D su sistemi CA ARCserve D2D è lenta. È possibile individuare altri sintomi quali:

- Il servizio Web di CA ARCserve D2D non risponde o occupa il 100% delle risorse della CPU.
- Prestazioni insufficienti o errore di comunicazione dei nodi di CA ARCserve D2D con il servizio Web.

Soluzione 1:

In alcune configurazioni di ambiente, il servizio Web di CA ARCserve D2D richiede tempi di CPU troppo lunghi oppure presenta un ritardo nella risposta. Per impostazione predefinita, Tomcat è configurato per allocare un valore limitato di memoria ai nodi, impostazione che potrebbe non essere adatta all'ambiente in uso. Per verificare questo problema, consultare i seguenti file di registro:

```
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stdout.*.log
<D2D_home>\TOMCAT\logs\casad2dwebsvc-stder.*.log
<D2D_home>\TOMCAT\logs\catalina.*.log
<D2D_home>\TOMCAT\logs\localhost.*.log
```

Individuare il seguente messaggio:

```
java.lang.OutOfMemoryError
```

Per correggere il problema, aumentare il valore di memoria allocata.

Per aumentare la memoria, eseguire le operazioni riportate di seguito:

1. Aprire l'Editor del Registro di sistema e selezionare la seguente chiave:
   - Sistemi operativi x86:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java`
   - Sistemi operativi x64:

     `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java`

2. Eseguire una delle seguenti operazioni:
   - Se il messaggio presente nel file di registro è il seguente:

     ```
     java.lang.OutOfMemoryError: PermGen space
     ```

     Aggiungere la stringa seguente al valore di Opzioni.

     ```
     -XX:PermSize=128M -XX:MaxPermSize=128M
     ```

     Nota: potrebbe essere necessario aumentare il valore di -XX:MaxPermSize per adattarlo al proprio ambiente.
   - Se il messaggio presente nel file di registro è uno dei seguenti:

     ```
     java.lang.OutOfMemoryError: Java heap space
     java.lang.OutOfMemoryError: GC overhead limit exceeded
     ```

     Aumentare il valore del seguente DWORD:

     ```
     JvmMx
     ```
3. Riavviare il servizio Web di CA ARCserve D2D.

Sintomo 2

I backup pianificati vengono ignorati e ne viene interrotta l'esecuzione.

Soluzione 2

Quando il valore massimo configurato corrisponde a 20 backup simultanei (o un valore inferiore), eseguire le seguenti operazioni:

1. Aumentare il valore del seguente DWORD:

   ```
   JvmMx=256
   ```

   Nota: il valore DWORD viene riportato nella soluzione 1.
2. Aggiungere la stringa seguente al valore di Opzioni.

   ```
   -XX:MaxPermSize=128M
   ```

   Nota: il valore DWORD viene riportato nella soluzione 1.

Quando il valore massimo configurato è compreso tra 20 e 50 backup simultanei, eseguire le seguenti operazioni:

1. Aumentare il valore del seguente DWORD:

   ```
   JvmMx=512
   ```

   Nota: il valore DWORD viene riportato nella soluzione 1.
2. Aggiungere la stringa seguente al valore di Opzioni.

   ```
   -XX:MaxPermSize=256M
   ```

   Nota: il valore DWORD viene riportato nella soluzione 1.

Errore di connessione di CA ARCserve Central Virtual Standby con il servizio Web di CA ARCserve D2D sui nodi remoti

Applicabile ai sistemi operativi Windows.

Sintomo:

CA ARCserve Central Virtual Standby non è in grado di stabilire la connessione con il servizio Web CA ARCserve D2D sui nodi remoti.

Soluzione:

La seguente tabella descrive i motivi per cui CA ARCserve Central Virtual Standby non è in grado di stabilire la connessione con il servizio Web di CA ARCserve D2D sui nodi remoti e indica le azioni correttive corrispondenti:

Causa	Misura correttiva
La rete non è disponibile o non è stabile durante l'applicazione dei criteri.	Verificare che la rete sia disponibile e stabile e riprovare.
Il computer di CA ARCserve D2D non è in grado di gestire il carico quando l'applicazione tenta di stabilire la comunicazione con il nodo.	Verificare che lo stato della CPU sul nodo di CA ARCserve D2D si normalizzi e riprovare.
Durante la distribuzione dei criteri, il servizio CA ARCserve D2D non è in esecuzione sul nodo remoto.	Verificare che CA ARCserve D2D sia in esecuzione sul nodo remoto e riprovare.
Si verificano problemi di comunicazione del servizio CA ARCserve D2D.	Riavviare il servizio CA ARCserve D2D sul nodo remoto e riprovare.

Viene visualizzato un errore del certificato quando si accede all'applicazione

Valido per piattaforme Windows.

Sintomo:

Quando si accede all'applicazione viene visualizzato il seguente messaggio nella finestra del browser:

- Internet Explorer

  `Si è verificato un problema con il certificato di protezione del sito Web.`

- Firefox

  `Questa connessione non è attendibile.`

- Chrome:

  `Il certificato di sicurezza di questo sito non è attendibile.`

Se si specifica un'opzione che consente di passare al sito Web, sarà possibile accedere all'applicazione. Questo comportamento, tuttavia, si verifica ogni volta che si accede all'applicazione.

Soluzione:

Questo comportamento si verifica quando si imposta l'utilizzo di HTTPS come protocollo di comunicazione. Per risolvere temporaneamente il problema, nella finestra del browser fare clic sul collegamento che consente di passare al sito Web. Al successivo accesso all'applicazione, comunque, il messaggio verrà nuovamente visualizzato.

Il protocollo di comunicazione HTTPS (sicuro) garantisce una maggiore sicurezza rispetto al protocollo di comunicazione HTTP. Se si desidera continuare a comunicare utilizzando il protocollo di comunicazione HTTPS, è possibile acquistare un certificato di sicurezza da VeriSign e quindi installare il certificato sul server applicazioni. Facoltativamente, è possibile impostare su HTTP il protocollo di comunicazione utilizzato dall'applicazione. Per impostare il protocollo di comunicazione su HTTP, procedere come segue:

1. Accedere al server in cui è installata l'applicazione.
2. Individuare la seguente directory:

   `C:\Programmi\CA\ARCserve Central Applications\BIN`

3. Eseguire il file batch seguente:

   `ChangeToHttp.bat`

4. Al termine dell'esecuzione del file batch, aprire Server Manager di Windows.

   Riavviare il seguente servizio:

   `Servizio CA ARCserve Central Applications`

Viene visualizzato un messaggio relativo a credenziali non valide durante l'aggiunta di nodi

Valido per piattaforme Windows.

Sintomo:

Quando si tenta di aggiungere nodi alla schermata Nodi, viene visualizzato il seguente messaggio:

```
Credenziali non valide.
```

Soluzione:

Questo problema si verifica nei seguenti casi:

- Le credenziali specificate nella finestra di dialogo Aggiungi nodi non sono corrette.
- L'orario sul nodo non corrisponde all'orario sul server applicazioni.

Per risolvere il problema, procedere come segue:

1. Accedere al server applicazioni e quindi accedere all'applicazione.
2. Dalla pagina principale, selezionare Nodo nella barra di navigazione.

   Verrà visualizzata la schermata Nodo.
3. Dalla barra degli strumenti Nodo, fare clic su clic Aggiungi, quindi selezionare Aggiungi nodo per IP/Nome dal menu di scelta rapida.

   Verrà visualizzata la finestra di dialogo Aggiungi nodo per IP/Nome.

4. Completare i seguenti campi:
   - **IP/Nome nodo** - Consente di specificare l'indirizzo IP o il nome del nodo.
   - **Descrizione** - Consente di specificare una descrizione per il nodo.
   - **Nome utente** - Consente di specificare il nome utente richiesto per l'accesso al nodo.
   - **Password** - Consente di specificare la password richiesta per l'accesso al nodo.

   Fare clic su Convalida.
5. Se viene visualizzato il messaggio Credenziali non valide, procedere come segue:
   a. Verificare di avere specificato le credenziali corrette nella finestra di dialogo Aggiungi nodi e quindi fare clic su Convalida.
   b. Se viene visualizzato il messaggio Credenziali non valide, assicurarsi che l'orario del sistema operativo del server applicazioni corrisponda all'orario del sistema operativo sul nodo.

      Nota: gli orari dei sistemi operativi possono appartenere a diversi fusi orari. Le date dei sistemi operativi, tuttavia, non possono essere diverse. In particolare, assicurarsi che la data del sistema operativo sul nodo non sia più di un giorno avanti o indietro rispetto alla data del sistema operativo sul server applicazioni.

Messaggi di credenziali non valide su Windows XP

Valido su computer con sistema operativo Windows XP.

Sintomo:

Quando vengono aggiunti nodi basati su Windows XP dalla schermata Nodo, viene visualizzato il seguente messaggio:

```
Credenziali utente non valide.
```

Soluzione:

In alcuni casi, CA ARCserve Central Virtual Standby non è in grado di aggiungere nodi Windows XP, se l'opzione di cartella Utilizza condivisione file semplice è stata selezionata. Per risolvere il problema, procedere come segue:

1. Accedere al nodo Windows XP e aprire Esplora risorse.
2. Scegliere Opzioni cartella dal menu Strumenti.

   Verrà visualizzata la finestra di dialogo Opzioni cartella.

3. Fare clic su Visualizza e selezionare Condivisione file semplice (scelta consigliata).
4. Deselezionare la casella di controllo accanto all'opzione Condivisione file semplice (scelta consigliata), quindi fare clic su OK.

   La condivisione file semplice viene disattivata.

5. Acceda al server CA ARCserve Central Virtual Standby e aggiungere il nodo.

Errore di accesso negato con l'aggiunta di un nodo per IP/Nome

Valido su tutti i sistemi operativi Windows con supporto del Controllo account utente (UAC).

Nota: Windows Vista o versioni successive.

Sintomo:

Se i nodi vengono aggiunti dalla finestra di dialogo Aggiungi nodo per IP/Nome utilizzando un account utente appartenente al gruppo di amministratori è diverso dall'account predefinito di amministratore o dall'account utente di dominio, viene visualizzato il messaggio seguente:

```
Accesso negato. Verificare di disporre dei privilegi di amministratore e che l'accesso al registro di sistema remoto non sia limitato dai criteri di protezione locali del computer aggiunto.
```

Come risultato non è possibile aggiungere il nodo.

Soluzione:

Si tratta di un comportamento previsto in caso di abilitazione del Controllo account utente (UAC) su un computer con sistema operativo Windows e supporto UAC. Il Controllo dell'account utente è una funzionalità Windows che consente l'accesso remoto al computer solo agli utenti con diritti di amministratore.

Per risolvere il problema, procedere secondo una delle modalità riportate a continuazione:

Disabilitare il controllo dell'account utente remoto:

1. Fare clic su Start, digitare regedit nel campo Cerca programmi e file e premere Invio per aprire l'editor del Registro di sistema di Windows.

   Nota: potrebbe essere necessario specificare le credenziali di amministratore per accedere all'editor del Registro di sistema di Windows.

2. Individuare e fare clic sulla chiave di registro seguente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. Dal menu Modifica, fare clic su Nuovo e selezionare Valore DWORD (32 bit).
4. Specificare LocalAccountTokenFilterPolicy come nome della nuova voce e premere Invio.
5. Fare clic con il tasto destro del mouse su LocalAccountTokenFilterPolicy e fare clic su Modifica.
6. Specificare 1 nel campo Dati valore e fare clic su OK.
7. Uscire dall'editor del Registro di sistema.

Disabilitare il Controllo dell'account utente:

1. Accedere al nodo utilizzando l'account amministratore.
2. Aprire il Pannello di controllo di Windows.
3. Aprire Account utente.

4. Nella schermata Modifica dell'account utente, fare clic su Modifica impostazioni di Controllo dell'account utente ed eseguire una delle operazioni seguenti:

   - **Windows Vista e Windows Server 2008:** nella schermata Modifica dell'account utente, fare clic su Attiva o disattiva Controllo account utente. Nella sezione Per aumentare la protezione del computer e renderlo più sicuro, attivare il controllo dell'account utente, deselezionare la casella di controllo accanto Per proteggere il computer, utilizzare il controllo dell'account utente e fare clic su OK.

     Riavviare il computer per applicare le modifiche apportate al Controllo dell'account utente.

   - **Windows Server 2008 r2 e Windows 7:** nella schermata Scegliere quando ricevere la notifica delle modifiche al computer, spostare l'Indicatore scorrevole da Notifica sempre a Non notificare mai. Fare clic su OK e chiudere il Pannello di controllo di Windows.

Riavviare il computer per applicare le modifiche apportate al Controllo dell'account utente.

I nodi non compaiono nella schermata Nodo dopo la modifica del nome del nodo

Valido per piattaforme Windows.

Sintomo:

Il nome host del nodo è stato modificato dopo l'aggiunta alla schermata Nodo. Il nodo non viene più visualizzato nella schermata Nodo.

Soluzione:

Si tratta di un comportamento normale. CA ARCserve Central Virtual Standby conserva il nome del nodo aggiunto dalla schermata Nodo. Quando si rinomina il nodo, Virtual Standby non è in grado di rilevare il nodo. Il nodo, pertanto, non viene visualizzato nella schermata Nodo.

Per visualizzare i nodi rinominati nella schermata Nodo, procedere come segue:

1. Rinominare il nodo.
2. Aprire la schermata Nodo ed eliminare il nodo (a pagina 67) rinominato.
3. Aggiungere il nodo (a pagina 33) utilizzando il nuovo nome.

Sistema operativo non trovato

Valido per piattaforme Windows.

Sintomo:

Il seguente messaggio viene visualizzato in caso di errore di attivazione del computer virtuale Virtual Standby.

```
Sistema operativo non trovato.
```

Soluzione:

Il comportamento descritto può inoltre verificarsi su computer virtuali contenenti periferiche SCSI e IDE. Se il problema si verifica, verificare la configurazione dei dischi sul computer virtuale e accertarsi che la sequenza di avvio del computer virtuale di cui è stato eseguito il recupero corrisponda all'origine del computer virtuale. Se la sequenza di avvio è differente, sarà necessario aggiornare il BIOS del computer virtuale di cui è stato eseguito il recupero corrispondente all'origine.

Nota: utilizzare (0:1) per rappresentare il primo disco IDE.

Errore dei processi Virtual Standby verso sistemi Hyper-V

Applicabile ai sistemi operativi Windows.

Sintomo:

Si verifica un errore dei processi Virtual Standby verso sistemi Hyper-V. Il seguente messaggio viene visualizzato nel Registro attività:

```
Impossibile acquisire il computer virtuale Hyper-V durante il processo Virtual
Standby.
```

Soluzione:

I processi Virtual Standby producono errori al verificarsi delle seguenti condizioni:

- Il servizio Web Virtual Standby non è in grado di recuperare informazioni relative al computer virtuale dal sistema Hyper-V. Si verificano problemi di comunicazione tra il server CA ARCserve Central Virtual Standby e il sistema Hyper-V quando i server Hyper-V richiesti non vengono eseguiti sul sistema Hyper-V.

  Soluzione: verificare che tutti i servizi Hyper-V siano in esecuzione sul sistema Hyper-V.

- Il sistema Hyper-V non dispone di spazio su disco sufficiente per la creazione del computer virtuale Virtual Standby o per la creazione di una snapshot del computer virtuale Virtual Standby.

  Soluzione: riconfigurare il sistema Hyper-V per liberare spazio su disco nel volume di sistema.

Nota: se vengono rilevate altre possibili cause, contattare il Supporto tecnico di CA.

Errore dei processi di standby virtuale causato da errori interni

Applicabile ai sistemi operativi Windows.

Sintomo 1:

I processi di standby virtuale producono errori. In Registro attività appare uno dei seguenti messaggi:

```
Impossibile convertire il disco virtuale
Si è verificato un errore interno. Contattare il Supporto tecnico di CA.
```

Inoltre, VDDK riporta il seguente messaggio di errore:

```
Errore sconosciuto.
```

Soluzione 1:

Per risolvere il problema, considerare quanto segue:

- Le operazioni di conversione potrebbero avere esito negativo se non si dispone di spazio su disco sufficiente nell'archivio dati specificato nel criterio Virtual Standby. VDDK restituisce questo messaggio in quanto l'API di VDDK non supporta la funzionalità che consente di rilevare la quantità di spazio disponibile sul disco dell'archivio dati. Per risolvere il problema, liberare lo spazio su disco dell'archivio dati originale necessario per il completamento dell'operazione, quindi inoltrare nuovamente il processo.
- I disturbi di rete ed un traffico di rete elevato possono comportare un errore dei processi di conversione. Per risolvere il problema, verificare che il nodo di origine e il sistema server ESX o vCenter siano in grado di comunicare attraverso la rete, quindi inviare nuovamente il processo.
- Possono verificarsi errori dovuti a connessioni multiple simultanee di processi di backup o recupero di computer virtuali verso sistemi server ESX o vCenter, comprese le connessioni vSphere SDK mediante il client VMware vSphere. Per correggere il problema, chiudere le connessioni non necessarie e inviare nuovamente il processo.

  Il problema è causato da una limitazione della connessione di VMware VDDK. I seguenti limiti del protocollo NFC (Network File Copy) si applicano:

  - ESX 4: 9 connessioni dirette, massimo
  - ESX 4 tramite server vCenter: 27 connessioni, massimo
  - ESXi 4: 11 connessioni dirette, massimo
  - ESXi 4 tramite server vCenter: 23 connessioni, massimo
  - ESXi 5: limitato da un buffer di trasferimento per tutte le connessioni NFC e applicato dall'host. La somma di tutti i buffer di connessione NFC a un host ESXi non può superare i 32 MB. 52 connessioni mediante il server vCenter, compreso il limite per host.

  Nota: le connessioni non possono essere condivise tra dischi. I valori massimi non sono applicabili a connessioni hot-add o SAN. Se il client NFC non si chiude correttamente, le connessioni possono rimanere aperte per dieci minuti.
- Esaminare le sezioni Attività ed Eventi del log client VMware vSphere per rilevare errori interni per un computer virtuale specifico. Correggere gli errori interni e inviare nuovamente il processo.

  Esempio: il file VMDK è utilizzato da un'altra applicazione o un'altra operazione. Per risolvere il problema, rilasciare il file e inviare nuovamente il processo.

Sintomo 2:

I processi di standby virtuale producono errori. In Registro attività appare uno dei seguenti messaggi:

```
Impossibile convertire il disco virtuale
Si è verificato un errore interno. Contattare il Supporto tecnico di CA.
```

Inoltre, VDDK riporta il seguente messaggio di errore:

```
L'apertura di vmdk ha prodotto un errore. File non trovato.
```

Soluzione 2:

Questo problema può verificarsi nei seguenti casi:

- VDDK non ha elaborato una snapshot correttamente.
- VDDK non ha eliminato una snapshot manualmente o interna al computer virtuale.

Per risolvere il problema, inviare nuovamente il processo. Se il processo produce nuovamente un errore, eliminare il computer virtuale di cui è stato eseguito il recupero e inviare nuovamente il processo.

Sintomo 3:

I processi di standby virtuale producono errori. In Registro attività appare uno dei seguenti messaggi:

```
Impossibile convertire il disco virtuale
Si è verificato un errore interno. Contattare il Supporto tecnico di CA.
```

Inoltre, VDDK riporta il seguente messaggio di errore:

```
Impossibile aprire vmdk o messaggio di errore di connessione del server
```

Soluzione 3:

Il problema è causato da una limitazione della connessione di VMware VDDK. I seguenti limiti del protocollo NFC (Network File Copy) si applicano:

- ESX 4: 9 connessioni dirette, massimo
- ESX 4 tramite server vCenter: 27 connessioni, massimo
- ESXi 4: 11 connessioni dirette, massimo
- ESXi 4 tramite server vCenter: 23 connessioni, massimo

Nota: le connessioni non possono essere condivise tra dischi. I valori massimi non sono applicabili a connessioni hot-add o SAN. Se il client NFC non si chiude correttamente, le connessioni possono rimanere aperte per dieci minuti.

Errore dei processi Virtual Standby mediante la modalità di trasporto hotadd

Valido per piattaforme Windows.

Sintomo:

Errore delle operazioni di recupero durante il recupero dei dati mediante la modalità di trasporto hotadd. Il seguente messaggio viene visualizzato nel Registro attività:

```
Errore sconosciuto. Contattare il supporto tecnico.
```

Inoltre, VDDK riporta il seguente messaggio di errore:

```
Errore sconosciuto.
```

Soluzione:

Errore delle operazioni di ripristino con la modalità di trasporto hotadd quando le impostazioni del disco non sono configurate correttamente.

Per configurare il disco, procedere come segue:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.

   Aprire la riga di comando di Windows.

2. Dalla riga di comando, immettere il seguente comando:

   ```
   diskpart
   ```

   Premere Invio.

   Digitare SAN, quindi premere Invio.

   Vengono visualizzati i criteri SAN correnti.

3. Digitare il seguente comando:

   ```
   SAN POLICY = OnlineAll
   ```

   Premere Invio.

   Il criterio SAN viene configurato in modo da non eseguire il montaggio automatico dei volumi SAN.

4. Per cancellare l'attributo di sola lettura di un determinato disco SAN, selezionare il disco dall'elenco, quindi immettere il seguente comando:

   `attribute disk clear readonly`

   Premere Invio.

5. Digitare exit, quindi premere Invio.

Il disco viene configurato e sarà possibile inoltrare nuovamente il processo. Se il processo riporta errori ancora una volta, montare i dischi hotadd manualmente utilizzando la gestione disco sul sistema proxy.

Per montare i dischi manualmente, procedere come segue:

1. Accedere al sistema proxy di backup mediante un account con privilegi di amministratore.

   Aprire il Pannello di controllo di Windows e fare doppio clic su Strumenti di amministrazione.

   Viene visualizzata la finestra di dialogo degli strumenti di amministrazione.

2. Dall'elenco Preferiti, fare doppio clic su Gestione computer.

   Viene visualizzata la finestra della Gestione computer.

3. Espandere Archiviazione, quindi fare clic sulla Gestione disco.

   Vengono visualizzati i dischi.

4. Fare clic con il tasto destro del mouse sul disco che si desidera montare, quindi fare clic su In linea.

   Il disco viene montato e sarà possibile inoltrare nuovamente il processo.

Processi Virtual Standby completati con messaggi di avviso che indicano che non è stata rilevata alcuna sessione

Valido per piattaforme Windows.

Sintomo:

I processi Virtual Standby vengono completati e viene visualizzato uno dei seguenti messaggio nel Registro attività:

`Nessuna sessione al termine del processo Virtual Standby`

`Impossibile rilevare le sessioni di backup sul server CA ARCserve D2D per la creazione di snapshot del punto di ripristino mediante Virtual Standby. Il server CA ARCserve D2D potrebbe non contenere sessioni di backup da convertire.`

Soluzione:

Verranno riscontrati i seguenti problemi al verificarsi delle seguenti condizioni:

- È stato utilizzato CA ARCserve Central Protection Manager per l'applicazione del criterio di backup di CA ARCserve D2D al nodo e a uno dei seguenti elementi:
  - Le impostazioni di origine del backup di CA ARCserve D2D sono state modificate dall'opzione Backup di volumi singoli all'opzione Backup dell'intero computer e un backup completo non è stato inviato o non è stato completato mediante le impostazioni di backup aggiornate dopo la distribuzione del criterio Virtual Standby al nodo.

    Soluzione: inviare un backup completo del nodo CA ARCserve D2D.
  - Le impostazioni di origine del backup di CA ARCserve D2D sono state modificate dall'opzione Backup dell'intero computer all'opzione Backup di volumi singoli dopo la distribuzione del criterio Virtual Standby al nodo.

    Soluzione: modificare le impostazioni di origine del backup di CA ARCserve D2D dall'opzione Backup di volumi singoli all'opzione Backup dell'intero computer, quindi inviare un backup completo del nodo CA ARCserve D2D.

Modalità di trasporto SAN non utilizzata dai processi di backup e recupero

Valido per piattaforme Windows.

Sintomo:

I processi di backup e recupero non utilizzano la modalità di trasporto SAN (a pagina 215). I processi tornano alla modalità di trasporto NBD (a pagina 215)o alla modalità di trasporto NBDSSL (a pagina 215). Il campo Modalità di trasporto della finestra di dialogo Monitoraggio dello stato di backup visualizza la modalità utilizzata.

Soluzione:

I sintomi descritti precedentemente possono verificarsi se SAN LUN non è configurato in modo appropriato nel sistema proxy di backup. Tuttavia, se la Gestione Disco di Windows rileva la presenza di SAN LUN e il problema persiste, il disco potrebbe non essere in linea o l'attributo di lettura del disco potrebbe non essere corretto. Riconfigurare il disco per impedire che questo comportamento si verifichi nuovamente.

Per configurare il disco, procedere come segue:

1. Accedere al nodo di origine del server di monitoraggio mediante un account con privilegi amministrativi.
2. Aprire la riga di comando di Windows.

3. Dalla riga di comando, immettere il seguente comando:

   ```
   diskpart
   ```

   Premere Invio.

4. Digitare SAN, quindi premere Invio.

   Vengono visualizzati i criteri SAN correnti.

5. Digitare il seguente comando:

   ```
   SAN POLICY = OnlineAll
   ```

   Premere Invio.

   Il criterio SAN viene configurato in modo da non eseguire il montaggio automatico dei volumi SAN.

6. Per cancellare l'attributo di sola lettura di un determinato disco SAN, selezionare il disco dall'elenco, quindi immettere il seguente comando:

   ```
   attribute disk clear readonly
   ```

   Premere Invio.

7. Digitare exit, quindi premere Invio.

Il disco viene configurato e sarà possibile inoltrare nuovamente il processo.

Errore di montaggio dei dischi in modalità trasporto hotadd dei processi di backup e recupero

Valido per piattaforme Windows.

Sintomo:

I processi di backup e ripristino che utilizzano la modalità di trasporto hotadd non possono eseguire il montaggio di dischi sul nodo di origine del server di monitoraggio. Viene inoltre visualizzato il seguente messaggio nel Registro attività:

```
Impossibile aprire il file VMDK %1!s!. Per ulteriori informazioni, consultare il registro di debug AFBackend.Log. Contattare il supporto tecnico.
```

Soluzione:

Per risolvere il problema, procedere come segue:

1. Aprire il client VMware vSphere.

   Accedere al sistema server ESX o al sistema server vCenter mediante le credenziali di amministratore.

2. Selezionare il computer virtuale proxy e modificare le impostazioni per il computer virtuale proxy.

3. Rimuovere i dischi hotadd dal sistema proxy (nel caso in cui siano stati associati dischi durante il processo di conversione).

4. Inoltrare nuovamente il processo.

Risoluzione problemi per numero di errore

La tabella seguente descrive i numeri di errore visualizzati come messaggi popup durante l'aggiunta o l'aggiornamento dei nodi mediante CA ARCserve Central Virtual Standby.

Numero errore	Descrizione	Soluzione possibile
12884901933	Impossibile stabilire una connessione con il servizio di CA ARCserve D2D su *** con numero di errore 12884901933. Verificare che tutte le voci del nodo siano corrette e che il servizio di CA ARCserve D2D sia in esecuzione.	Verificare che: ■ Il servizio di CA ARCserve D2D sia in esecuzione sul nodo. ■ Il nome host, l'indirizzo IP e il protocollo di comunicazione specificati per il nodo siano corretti. ■ Il servizio Web di CA ARCserve D2D sul nodo sia in esecuzione e non bloccato a causa si un errore di risoluzione dell'indirizzo IP del nodo da parte del DNS. ■ Il servizio Web di CA ARCserve D2D sul nodo sia in esecuzione e il firewall di Windows, o qualsiasi altro firewall, non stiano bloccando la comunicazione. ■ Il cavo di rete connesso al nodo stia funzionando correttamente. ■ L'utente che accede al nodo disponga delle autorizzazioni richieste per la comunicazione mediante una rete senza fili.

Collegamento Aggiungi nuova scheda non funzionante per Internet Explorer 8, 9 e Chrome.

Valido per Windows

Sintomo:

Quando viene aggiunto un nuovo collegamento alla scheda della barra di navigazione specificando un URL HTTPS, facendo clic sulla nuova scheda verranno visualizzati i seguenti messaggi di errore:

- Internet Explorer 8 e 9:

  `Il contenuto è stato bloccato poiché non è stato firmato da un certificato di protezione valido.`

- Chrome:

  `La pagina Web non è disponibile.`

Soluzione:

Per correggere il problema relativo a Internet Explorer, eseguire le seguenti operazioni:

- Internet Explorer 8:

  Fare clic sulla barra del messaggio e selezionare Visualizza contenuto bloccato.

- Internet Explorer 9:

  Fare clic sul pulsante Mostra il contenuto della Barra messaggi nella parte inferiore della pagina. La pagina viene aggiornata e il collegamento alla scheda aggiunta viene aperto correttamente.

Per risolvere il problema relativo a Chrome, eseguire le seguenti operazioni:

Fase 1 - Esportazione del certificato:

1. Aprire una nuova scheda in Chrome ed immettere l'URL HTTPS.

   Verrà visualizzato il messaggio di avviso "Il certificato di sicurezza del sito non è affidabile!"

2. Dalla barra degli indirizzi, fare clic sul lucchetto contrassegnato con una X.

   Verrà visualizzata una finestra popup contenente il collegamento a Informazioni sul certificato.

3. Fare clic sul collegamento Informazioni sul certificato.

   Verrà visualizzata la finestra di dialogo Certificato.

4. Fare clic sulla scheda Dettagli, quindi selezionare Copia su file per salvare il certificato sul computer locale.

   Viene visualizzata la procedura guidata di esportazione del certificato.

5. Fare clic su Avanti per selezionare il formato desiderato per l'esportazione del file.

   Nota: X.509 binario codificato DER (.CER) è selezionato per impostazione predefinita.

6. Fare clic su Avanti per selezionare un percorso in cui salvare il certificato.
7. Fare clic su Avanti per completare la procedura guidata di esportazione del certificato, quindi fare clic su Fine.

Il certificato viene esportato correttamente.

Fase 2 - Importazione del certificato:

1. Selezionare Opzioni da Personalizza e controlla Google Chrome.

   Verrà visualizzata la finestra di dialogo Opzioni.

2. Selezionare l'opzione Roba da smanettoni, quindi selezionare Gestisci certificati della sezione HTTPS/SSL.

   Viene visualizzata la finestra di dialogo Certificati.

3. Fare clic su Importa.

   Viene visualizzata la procedura guidata di importazione del certificato.

4. Fare clic su Avanti per ricercare il certificato salvato sul computer locale.
5. Fare clic su Avanti per aprire l'Archivio certificati.

   Verrà visualizzata la finestra di dialogo Archivio certificati.

6. Fare clic su Sfoglia per aprire la finestra di dialogo Selezione archivio certificati.

   Viene visualizzata la finestra di dialogo Selezione archivio certificati.

7. Selezionare Autorità di certificazione fonti attendibili dall'elenco di file, quindi fare clic su OK.

   Viene visualizzata la finestra di dialogo Archivio certificati.

8. Fare clic su Avanti per completare la procedura guidata di importazione del certificato, quindi fare clic su Fine.

   Verrà visualizzata una finestra di dialogo di avviso che comunica all'utente che si sta per installare un certificato.

   Fare clic su Sì per accettare i termini.

Il certificato viene importato correttamente.

Collegamento Aggiungi nuova scheda, Feed RSS e commenti relativi al social network non avviati correttamente in Internet Explorer 8 e 9

Valido per Windows

Sintomo:

Per un URL CA ARCserve Central Applications HTTPS:

Quando viene aggiunto un nuovo collegamento alla scheda della barra di navigazione specificando un URL HTTP, facendo clic sulla nuova scheda e sul collegamento Commenti e suggerimenti verranno visualizzati i seguenti messaggi di errore:

```
La navigazione alla pagina Web è stata annullata.
```

Inoltre, i feed RSS non vengono visualizzati.

Nota: il collegamento Commenti e suggerimenti visualizza un messaggio di errore anche se non viene aggiunto il collegamento alla nuova scheda.

Soluzione:

Per risolvere il problema, procedere come segue:

- Internet Explorer 8:

  Dopo aver eseguito l'accesso, viene visualizzato il messaggio di avviso Visualizzare solo le informazioni della pagina Web fornite in modo protetto? Selezionare No per visualizzare il contenuto non protetto della pagina Web.

- Internet Explorer 9:

  Fare clic sul pulsante Mostra tutto il contenuto della barra dei messaggi nella parte inferiore della pagina. La pagina viene aggiornata e il collegamento alla scheda aggiunta viene aperto correttamente.

Impossibile specificare un asterisco o un carattere di sottolineatura come carattere jolly nei campi di filtro utilizzando la tastiera giapponese

Valido per Windows

Sintomo:

A causa di una differenza di codici con le tastiere giapponesi, non è possibile immettere il carattere jolly "*" e altri caratteri speciali, come ad esempio il carattere di sottolineatura "_" nei seguenti campi di filtro:

- Il problema si verifica soltanto con Firefox:
  - Nodo > Aggiungi gruppo - Campo Filtro Nome nodo
  - Criteri > Scheda Assegnazione criterio > Assegnazione e annullamento assegnazione del criterio - Campo Filtro Nome nodo.
  - Ripristina > Esplorazione nodi - Campo Nome nodo

Soluzione:

- Per impedire che si verifichi il problema, aprire un'applicazione di modifica del testo come ad esempio Notepad. Digitare i caratteri speciali (ad esempio "*" e "_") nell'editor di testo. Copiare quindi i caratteri dall'editor di testo nel campo.

Errore durante l'avvio automatico dei computer virtuali

Valido per Windows

Sintomo:

I computer virtuali non vengono avviati automaticamente. I valori di recupero Impostazioni di sostituzione sono definiti su Avvia il computer virtuale automaticamente.

Soluzione:

Si tratta di un comportamento previsto. L'applicazione non è in grado di attivare automaticamente i computer virtuali aggiunti dai server CA ARCserve Central Host-Based VM Backup. Di conseguenza, quando si esegue la distribuzione dei criteri con metodo di recupero impostato su Avvia il computer virtuale automaticamente sui nodi protetti da backup dei computer virtuali basato sull'host, Virtual Standby modifica il metodo di recupero su Avvia il computer virtuale manualmente.

Per risolvere questo comportamento, attivare la protezione del computer virtuale con CA ARCserve D2D o CA ARCserve Central Protection Manager.

Errore della comunicazione tra CA ARCserve Central Virtual Standby e i nodi

Valido per i sistemi operativi Windows

Sintomo:

CA ARCserve Central Virtual Standby non è in grado di stabilire la connessione con i nodi.

Soluzione:

Per garantire che CA ARCserve Central Virtual Standby possa eseguire la distribuire i criteri sui nodi e di proteggere i nodi, verificare che il server e i nodi di Virtual Standby che si desidera proteggere siano in grado di comunicare l'uno con l'altro utilizzando i nomi host.

Procedere come descritto di seguito:

1. Dal server CA ARCserve Central Virtual Standby, eseguire il ping dei nodi da proteggere utilizzando i nomi host dei nodi.
2. Dai nodi che si desidera proteggere, eseguire il ping di CA ARCserve Central Virtual Standby utilizzando il nome host del server.

Errore durante la preparazione della conversione remota. Impossibile creare la snapshot VSS

Valido per tutti i sistemi operativi Windows

Sintomo:

Durante la creazione manuale di una snapshot VSS con l'utilità vssadmin, viene visualizzato il seguente messaggio di errore:

È già in corso la creazione di un'altra copia shadow. Attendere alcuni istanti e riprovare.

Soluzione:

Riavviare il servizio della copia shadow del volume

Capitolo 9: Procedura consigliata

Questa sezione contiene i seguenti argomenti:

Impatto del processo di installazione sui sistemi operativi

Il processo di installazione di CA ARCserve Central Applications aggiorna i vari componenti del sistema operativo Windows utilizzando un modulo di installazione denominato MSI (Microsoft Installer Package). I componenti inclusi nel file MSI consentono a CA ARCserve Central Applications di eseguire operazioni personalizzate che permettono di installare, aggiornare o disinstallare CA ARCserve Central Applications.

Nella tabella seguente vengono descritte le azioni personalizzate e i componenti interessati.

Nota: tutti i pacchetti MSI di CA ARCserve Central Applications richiamano i componenti elencati in questa tabella quando si installa e disinstalla CA ARCserve Central Applications.

Componente	Descrizione
CallAllowInstall	Consente al processo di installazione di verificare le condizioni relative all'installazione corrente dell'applicazione.
CallPreInstall	Consente al processo di installazione di eseguire la lettura e la scrittura delle proprietà del pacchetto MSI. Ad esempio, la lettura del percorso di installazione dell'applicazione dal pacchetto MSI.
CallPostInstall	Consente al processo di installazione di eseguire varie operazioni relative all'installazione. Ad esempio,la registrazione dell'applicazione nel Registro di sistema di Windows.
CallAllowUninstall	Consente al processo di disinstallazione di verificare le condizioni relative all'installazione corrente dell'applicazione.
CallPreUninstall	Consente al processo di disinstallazione di eseguire varie operazioni relative alla disinstallazione. Ad esempio, l'annullamento della registrazione dell'applicazione dal Registro di sistema di Windows.

Componente	Descrizione
CallPostUninstall	Consente al processo di disinstallazione di eseguire varie attività dopo la disinstallazione dei file installati. Ad esempio, la rimozione dei file restanti.
ShowMsiLog	Consente di visualizzare il file di registro di Windows Installer in Notepad se si seleziona la casella di controllo Mostra registro di Windows Installer nelle finestre di dialogo di completamento dell'installazione, di errore dell'installazione o di interruzione dell'installazione. Sarà quindi necessario fare clic su Fine. (funziona solo con Windows Installer 4.0.)
ISPrint	Stampa il contenuto di un controllo ScrollableText in una finestra di dialogo. Azione personalizzata del file .dll di Windows Installer. Il nome del file DLL è SetAllUsers.dll e il punto di ingresso è PrintScrollableText.
CheckForProductUpdates	Utilizza FLEXnet Connect per verificare la disponibilità di aggiornamenti di prodotto. Questa azione personalizzata avvia un file eseguibile denominato Agent.exe e trasmette la seguente istruzione: /au[ProductCode] /EndOfInstall
CheckForProductUpdatesOnReboot	Utilizza FLEXnet Connect per verificare la disponibilità di aggiornamenti di prodotto al riavvio. Questa azione personalizzata avvia un file eseguibile denominato Agent.exe e trasmette la seguente istruzione: /au[ProductCode] /EndOfInstall /Reboot

- **Directory aggiornate** - Per impostazione predefinita, il processo di installazione installa e aggiorna i file dell'applicazione nelle seguenti directory:

  `C:\Program Files\CA\`*<application name> (ad esempio, ARCserve Central Applications o ARCserve D2D)*

  È possibile installare l'applicazione nella directory di installazione predefinita oppure in una directory alternativa. Il processo di installazione copia vari file di sistema nella directory seguente:

  `C:\WINDOWS\SYSTEM32`

- **Aggiornamento delle chiavi del Registro di sistema di Windows** - Durante il processo di installazione vengono aggiornate le seguenti chiavi del Registro di sistema di windows:

  Chiavi predefinite del Registro di sistema:

  HKLM\SOFTWARE\CA\<*application name*> *(ad esempio, ARCserve Central Applications o ARCserve D2D)*

  Il processo di installazione modifica e crea nuove chiavi del Registro di sistema, in base alla configurazione del sistema in uso.

- **Applicazioni installate** - Il processo di installazione installa le seguenti applicazioni nel computer in uso:
  - CA Licensing
  - Microsoft Visual C++ 2010 SP1 Redistributable
  - Java Runtime Environment (JRE) 1.7.0_06
  - Tomcat 7.0.29

File binari con informazioni non corrette sulla versione dei file

CA ARCserve Central Applications esegue l'installazione di file binari sviluppati da terze parti, altri prodotti CA, e CA ARCserve Central Applications contenenti informazioni sulla versione dei file incorrette. La seguente tabella descrive tali file binari.

Nome file binario	Origine
UpdateData.exe	CA License
zlib1.dll	Zlib Compression Library

File binari non contenenti il manifesto integrato

CA ARCserve Central Applications installa i file binari sviluppati da terze parti, altri prodotti CA Technologies, e file CA ARCserve Central Applications non contenenti un manifesto integrato o un manifesto di testo. La seguente tabella descrive tali file binari.

Nome file binario	Source (Origine)
BaseLicInst.exe	CA License
UpdateData.exe	CA License
vcredist_x64.exe	Microsoft

Nome file binario	Source (Origine)
vcredist_x86.exe	Microsoft
tomcat7.exe	Tomcat

File binari che richiedono un livello di privilegi di tipo Amministratore nel manifesto

CA ARCserve Central Applications installa file binari sviluppati da terze parti, da altri prodotti CA Technologies e file CA ARCserve Central Applications che richiedono un livello di privilegi di tipo Amministratore o più elevato. Per poter eseguire i servizi, i componenti e le applicazioni di CA ARCserve Central Applications è necessario effettuare l'accesso utilizzando un account amministrativo o un account che dispone di autorizzazioni più elevate. I file binari corrispondenti a tali servizi, componenti e applicazioni includono funzionalità specifiche di CA ARCserve Central Applications non disponibili per un account utente di base. Ne consegue che per completare un'operazione in Windows verrà richiesto di confermare tale operazione mediante l'immissione di una password oppure mediante l'utilizzo di un account che dispone di privilegi di amministrazione.

- **Privilegi di amministratore:** un profilo o un account amministrativo con privilegi di amministratore dispongono di autorizzazioni di lettura, scrittura ed esecuzione per tutte le risorse di sistema e di Windows. Se non si dispone di privilegi di amministratore, verrà richiesto di immettere il nome utente e la password di un utente con tali privilegi per poter continuare.
- **Privilegi più elevati disponibili:** un account con i privilegi più elevati disponibili consiste in un account utente di base e in un account utente avanzato eseguiti con privilegi di amministratore.

La seguente tabella descrive tali file binari.

Nome file binario	Origine
APMSetupUtility.exe	CA ARCserve Central Applications
ArcAppUpdateManager.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications
CA ARCserve Central ApplicationsPMConfigSettings.exe	CA ARCserve Central Applications
CCIConfigSettings.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
CfgUpdateUtil.exe	CA ARCserve Central Applications
D2DAutoUpdateUninstallUtility.exe	CA ARCserve Central Applications

Nome file binario	Origine
D2DPMConfigSettings.exe	CA ARCserve Central Applications
D2DUpdateManager.exe	CA ARCserve Central Applications
DBConfig.exe	CA ARCserve Central Applications
FWConfig.exe	CA ARCserve Central Applications
RemoteDeploy.exe	CA ARCserve Central Applications
RestartHost.exe	CA ARCserve Central Applications
SetupComm.exe	CA ARCserve Central Applications
SetupFW.exe	CA ARCserve Central Applications
SetupWrapper.exe	CA ARCserve Central Applications
Uninstall.exe	CA ARCserve Central Applications
UpdateInstallCommander.exe	CA ARCserve Central Applications
UpgradeDataSyncupUtility.exe	CA ARCserve Central Applications
jbroker.exe	Java Runtime Environment
jucheck.exe	Java Runtime Environment

Esclusione di file dalla scansione antivirus

Il software antivirus può compromettere la corretta esecuzione di dell'applicazione bloccando temporaneamente l'accesso ai file o mettendo in quarantena ed eliminando i file classificati erroneamente come sospetti o pericolosi. È possibile configurare la maggior parte dei software antivirus per escludere determinati processi, file o cartelle affinché non venga eseguita l'analisi di dati che non necessitano di protezione. La corretta configurazione del software antivirus è fondamentale per evitare che interferisca con le operazioni di backup e ripristino o con qualsiasi altro processo.

I seguenti processi, cartelle e file dovranno essere esclusi dall'analisi anti-virus:

- Elenco di processi
  - C:\Programmi\CA\ARCserve Central Applications\BIN\CCIConfigSettings.exe
  - C:\:\Programmi\CA\ARCserve Central Applications\BIN\CfgUpdateUtil.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\DBConfig.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetApplicationDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetVolumeDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\VixGetApplicationDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\VixGetVolumeDetails.exe
  - C:\Programmi\CA\ARCserve Central Applications\BIN\GetApplicationDetails64.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\Asremsvc.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\CheckProdInfo.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\DeleteMe.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\SetupComm.exe
  - C:\Programmi\CA\ARCserve Central Applications\Deployment\RestartHost.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\D2DAutoUpdateUninstallUtility.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\D2DPMConfigSettings.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\D2DUpdateManager.exe
  - C:\Programmi\CA\ARCserve Central Applications\Update Manager\UpgradeDataSyncupUtility.exe

- C:\Programmi\CA\ARCserve Central Applications\TOMCAT\BIN\tomcat7.exe
- C:\Programmi\CA\ARCserve D2D\TOMCAT\JRE\jre7\bin
  - java.exe
  - java-rmi.exe
  - javaw.exe
  - keytool.exe
  - rmid.exe
  - rmiregistry.exe
- C:\Programmi(x86)\CA\SharedComponents\CA_LIC
  - CALicnse.exe
  - CAminfo.exe
  - CAregit.exe
  - ErrBox.exe
  - lic98log.exe
  - lic98Service.exe
  - lic98version.exe
  - LicDebug.exe
  - LicRCmd.exe
  - LogWatNT.exe
  - mergecalic.exe
  - mergeolf.exe

Per garantire il corretto funzionamento di CA ARCserve Central Virtual Standby e di Virtual Standby remoto, escludere i file seguenti che hanno come destinazione computer virtuali Hyper-V e processi Hyper-V:

1. Directory dei file di configurazione del computer virtuale:
   - (Valore predefinito) C:\Programmi\Microsoft\Windows\Hyper-V
   - Directory dei file di configurazione del computer virtuale CA ARCserve Central Virtual Standby:
2. Directory dei file del disco rigido del computer virtuale:
   - (Valore predefinito) C:\Utenti\Pubblica\Documenti pubblici\Hyper-V\Virtual Hard Disks
   - Directory dei file del disco rigido del computer virtuale CA ARCserve Central Virtual Standby:
3. Directory di file di snapshot:

- (Valore predefinito) %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots
- Directory dei file di snapshot del computer virtuale CA ARCserve Central Virtual Standby:

4. Processo Hyper-V:
   - %windows%\system32\Vmms.exe
   - %windows%\system32\Vmwp.exe

Modalità di concessione della licenza di CA ARCserve Central Virtual Standby

CA ARCserve Central Virtual Standby contiene le licenze seguenti:

- CA ARCserve Central Virtual Standby-Fisico
- CA ARCserve Central Virtual Standby-VMware
- CA ARCserve Central Virtual Standby-Hyper-V

Tutte le licenze sono basate su meccanismi di conteggio. CA ARCserve Central Virtual Standby verifica e concede le licenze per i nodi di CA ARCserve D2D in base ai seguenti criteri:

- Le licenze CA ARCserve Central Virtual Standby-Fisico vengono applicate a tutti i nodi di CA ARCserve D2D aggiunti per Nome/indirizzo IP o importati da file. CA ARCserve Central Virtual Standby concede le licenze CA ARCserve Central Virtual Standby-Fisico ai nodi dopo l'applicazione di un criterio e l'avvio del processo di conversione virtuale.

  Nota: questo è il comportamento predefinito per le licenze di CA ARCserve Central Virtual Standby.

- Le licenze CA ARCserve Central Virtual Standby-VMware vengono applicate a tutti i nodi di CA ARCserve D2D aggiunti per Nome/Indirizzo IP o importati da file e corrispondenti a computer virtuali VMware che risiedono su sistemi server ESX o vCenter. Ad ogni modo, prima di poter applicare licenze CA ARCserve Central Virtual Standby-VMware ai nodi, è necessario associare i nodi ad un sistema server ESX o vCenter specifico.

  Nota: per ulteriori informazioni, consultare la sezione Definizione di sistemi server ESX o vCenter per nodi VMware (a pagina 59).

  Le licenze CA ARCserve Central Virtual Standby-VMware vengono concesse a ciascun sistema server ESX dopo l'applicazione di un criterio ai nodi e l'avvio del processo di conversione virtuale.

- CA ARCserve Central Virtual Standby applica le licenze CA ARCserve Central Virtual Standby-VMware a tutti i nodi del computer virtuale importati da un sistema CA ARCserve Central Host-Based VM Backup. Le licenze CA ARCserve Central Virtual Standby-VMware vengono concesse ai nodi del computer virtuale dopo l'applicazione di un criterio ai nodi e l'avvio del processo di conversione virtuale.
- Le licenze CA ARCserve Central Virtual Standby-Hyper-V vengono applicate a tutti i nodi di CA ARCserve D2D aggiunti per Nome/Indirizzo IP o importati da file e che risiedono su un hypervisor Hyper-V. CA ARCserve Central Virtual Standby rileva la presenza del server Hyper-V quando si procede all'aggiunta dei nodi per Nome/ Indirizzo IP o all'importazione dei nodi da un file. Le licenze CA ARCserve Central Virtual Standby-Hyper-V vengono, quindi, concesse ai nodi di CA ARCserve D2D dopo l'aggiunta per Nome/Indirizzo IP o l'importazione da file.

Meccanismo di conteggio

La tabella seguente descrive il numero di licenze di CA ARCserve Central Virtual Standby richieste per un determinato scenario.

Tipo di nodo D2D	Licenza richiesta	Meccanismo di conteggio
Nodo fisico	CA ARCserve Central Virtual Standby-Fisico	Una licenza per nodo
Computer virtuale VMware	CA ARCserve Central Virtual Standby-VMware	Una licenza per ogni sistema server ESX/vCenter
Computer virtuale Hyper-V	CA ARCserve Central Virtual Standby-Hyper-V	Una licenza per ciascun sistema Hyper-V

Esempi:

- CA ARCserve Central Virtual Standby protegge cinque nodi fisici di CA ARCserve D2D. Sono necessarie cinque licenze CA ARCserve Central Virtual Standby-Fisico.
- CA ARCserve Central Virtual Standby protegge tre computer virtuali VMware che risiedono su un sistema server ESX. È necessaria una licenza CA ARCserve Central Virtual Standby-VMware.
- CA ARCserve Central Virtual Standby protegge 100 computer virtuali VMware distribuiti su dieci sistemi server ESX. Sono necessarie dieci licenze CA ARCserve Central Virtual Standby-VMware.
- CA ARCserve Central Virtual Standby protegge 20 computer virtuali Hyper-V distribuiti su cinque sistemi Hyper-V. Sono necessarie cinque licenze CA ARCserve Central Virtual Standby-Hyper-V.

- CA ARCserve Central Virtual Standby protegge tre computer virtuali Hyper-V che risiedono su un sistema Hyper-V e tre computer virtuali VMware che risiedono su un sistema server ESX. È necessaria una licenza CA ARCserve Central Virtual Standby-VMware e una licenza CA ARCserve Central Virtual Standby-Hyper-V.
- CA ARCserve Central Virtual Standby protegge cinque computer virtuali VMware importati da CA ARCserve Central Host-Based VM Backup che risiedono su un sistema server ESX. È necessaria una licenza CA ARCserve Central Virtual Standby-VMware.

Glossario

Conversione virtuale

La conversione virtuale è il processo utilizzato da CA ARCserve Central Virtual Standby per convertire i punti di ripristino di CA ARCserve D2D da nodi di origine in file di dati del computer virtuale, denominati snapshot del punto di ripristino.

Criterio

Un criterio è un insieme di specifiche per la protezione di un nodo in uno o più CA ARCserve Central Applications.

Gruppo nodo

Un gruppo nodo è un metodo in base al quale tutti i nodi gestiti da uno o più CA ARCserve Central Applications possono essere organizzati, ad esempio in base allo scopo, al sistema operativo o alle applicazioni installate.

Heartbeat

Un heartbeat è un segnale elettronico inviato dai nodi di origine al server di monitoraggio per identificare lo stato del nodo.

Modalità di trasporto HOTADD

La modalità di trasporto HOTADD è un metodo di trasporto dei dati che consente di eseguire il backup dei computer virtuali configurati con dischi SCSI. Per ulteriori informazioni, consultare la guida alla programmazione Virtual Disk API Programming Guide disponibile sulla pagina Web di VMware.

Modalità di trasporto NBD

La modalità di trasporto Network Block Device (NBD), denominata anche modalità di trasporto LAN, utilizza il protocollo NFC (Network File Copy) per la comunicazione. Diverse operazioni VDDK e VCB utilizzano una connessione per ciascun disco virtuale a cui effettuano l'accesso su ciascun server host ESX/ESXi, durante l'utilizzo di NDB.

Modalità di trasporto NBDSSL

La modalità di trasporto NBDSSL (Network Block Device Secure Sockets Layer) utilizza il protocollo di comunicazione NFC (Network File Copy). NBDSSL esegue il trasferimento dei dati crittografati mediante le reti di comunicazione TCP/IP.

Modalità di trasporto SAN

La modalità di trasporto SAN (Storage Area Network) consente il trasferimento dei dati di backup da sistemi proxy connessi alla rete SAN a periferiche di archiviazione mediante la comunicazione Fibre Channel.

Nodo

Un nodo è un computer fisico o virtuale gestito da uno o più CA ARCserve Central Applications.

Punto di ripristino

Un punto di ripristino è un'immagine di backup costituita da blocchi parent-plus-oldest-child. I backup secondari sono uniti ai backup principali per creare nuove immagini di punto di ripristino in modo che il valore specificato sia sempre aggiornato.

Server di monitoraggio

Un server di monitoraggio è un server che consente di verificare lo stato dei server di origine negli ambienti CA ARCserve Central Virtual Standby.

Snapshot del punto di ripristino

Una snapshot del punto di ripristino è un file del disco virtuale VMware (VMDK) o del disco rigido virtuale di Microsoft (VHD), che CA ARCserve Central Virtual Standby crea dai punti di ripristino di CA ARCserve D2D. CA ARCserve Central Virtual Standby consente di attivare i computer virtuali mediante snapshot del punto di ripristino in caso di errore dei server di origine di CA ARCserve D2D dell'ambiente di produzione.